Comparative Analysis of High-Volume Decentralised Cryptocurrency Exchanges

Elden Ren, **Vikhyath Mondreti**, **Rahul Shah**, **Aditya Prasad**, **Samarth Goel**

ABSTRACT

Decentralized Exchanges (DEX) allow P2P transactions without any intermediaries. In many ways, these protocols solve a problem at the center of the modern-day financial system with average trading volumes now reaching billions of dollars daily. However, at present, there is not yet a precise and approachable methodology for evaluating a modern DEX. We offer a systematic aggregation of key metrics and expert perspectives to compare the core aspects of the most popular exchanges. With these novel insights, we aim to build a trader-focused recommendation model that quantitatively predicts the optimal sequence or procedure of transactions and exchanges to maximize returns on a cryptocurrency swap.

1. Introduction and Problem Definition

The problem we are seek to solve consists of two core components:

■ Produce a clear, novel quantitative comparison of the highest volume decentralized exchanges today.

■ Create a data-driven system built on the market making mechanisms various decentralized exchanges to calculate the optimal sequence of trades to perform a swap.

We want to explore the ecosystem of decentralized exchanges from a trader's perspective, in the process proposing a model that could potentially allow non-technical players to participate in the broader cryptocurrency economy. In this paper, we build a knowledge framework to accurately describe and compare prominent decentralized exchanges and design a system that uses this information (along with data points from exchange APIs) to effectively execute or recommend swaps.

2. Related Works

In addition to the whitepapers of each of the exchange protocols, there were three related works that offered solid foundations for the analyses conducted in this paper.

2.1 *Decentralized Exchanges with Automated Market Maker Protocols*

In this 2021 SoK, Xu et al. establish a a general AMM framework describing the economics (liquidity, staking and security rewards, governance rights, swap fees, gas fees, etc) and formalizing the system's state-space representation. More pertinent is their comprehensive comparison of top AMM protocols through popular metrics such as the conservation, slippage and loss functions. In effect, the most useful aspect of this closely related work was the remarkably detailed review covering both DeFi and traditional market microstructures.

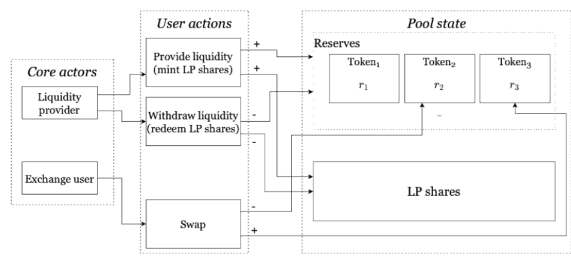

Fig. 1. AMM Mechanism (Xu et al., 2021)

2.2 *The Adoption of Blockchain-Based Decentralized Exchanges*

Second, we have this paper by Capponi and Jia also written this year. This was chosen due to its significantly higher focus on the trader's perspective, and clear related statements on behavioral assumptions. The overarching theme of the work is the use of a game theoretical model to answer questions pertaining to liquidity incentives. More specifically, they talk about whether an incentive structure exists at all for providing liquidity, transaction breakdown points if the AMM's reserves are drained, and generally which tokens are more suitable for these protocols. They finally argue that gas fees don't sidestep the arbitrage problem and evidently form the bottleneck for wider adoption.

2.3 *Deconstructing Decentralized Exchanges*

Finally, we have an essay by blockchain law and policy expert Lindsay Lin that delves into the larger architectural structure, in more non-mathematical terms, of decentralized exchanges. She describes these micro-structural components to be the blockchain platform, counterparty discovery mechanism, order matching algorithm, and transaction settlement protocol. More interestingly, the performance and security challenges faced by different architectural choices are also covered. It describes in reasonable detail how regulatory forces against centralization have in turn driven DEXs' growth which offer advantages such as more private transactions as well as access to less liquid or riskier crypto assets.

3. Approach

In our research, we focus on the market making mechanisms of each decentralized exchange, detailed in their whitepapers, as well as other publicly available metrics such as transaction costs, liquidity/trade volumes, and latency. These data-points can be combined with popular current perspectives in the decentralized finance community to get a more holistic view of the DEX landscape and motivate the strategies of cryptocurrency traders. This paper will comprehensively compare the following high volume exchanges:

Uniswap V3 **PancakeSwap V2** **dYdX**
Curve **Sushiswap**

In order to produce standardized metrics for comparing these exchanges, we will primarily examine Bitcoin-Ethereum exchanges under the framework of each DEX. To collect data, we fork a block in Hardhat and call the smart contracts of the various DEXs on the block to observe their behavior. In addition, we use blockchain explorer tools including Etherscan and BscScan to collect transaction data and other information to guide our research. After outlining and analyzing the key differences between these decentralized exchanges, we detail the design of a system that can model the behavior of each of these DEXs to effectively perform cryptocurrency swaps.

4. Evaluation

4.1 Analysis of Market Making Mechanisms and Reward Structures

As mentioned in the literature review, the design of a DEX heavily influences the decision-making of users, who impact the liquidity and volume of the exchange, ultimately determining the success or failure of a DEX. The primary point of differentiation between major decentralized exchanges is the market making mechanisms. Of the 5 DEX discussed in this paper, 4 of them (Uniswap, Sushiswap, Pancakeswap, and Curve) are AMM-based, and just 1 (dydx) is an order book-based exchange. In this section, we outline the differences between the respective market making mechanisms of each of the DEXs of interest (listed in the table below), and we summarize the advantages and disadvantages presented by their distinct attributes. Besides analyzing market making mechanisms, we also discuss the frameworks used by each DEX to attract more liquidity and volume to their respective platforms.

Table 1. DEX Market Makers

DEX	Mechanism
Sushiswap	$xy = k$
Uniswap V3	$(x + \frac{L}{\sqrt{p_b}})(y + L\sqrt{p_a}) = L^2$
Curve V2	$KD^{N-1}\sum x_i + \prod x_i = KD^N + (\frac{D}{N})^N$
Pancakeswap	$AD^{N-1}\sum x_i + \prod (Dw_i)^{Nw_i} = AD^N + \prod (\frac{D^2 w_i^2}{x_i})^{Nw_i}$
dYdX	Order Book

4.1.1 Sushiswap

Sushiswap is a DEX built on ethereum and is based around SUSHI, an ERC-20 token. Sushiswap uses the constant product market maker formula, which was first introduced by Uniswap. The key distinction between Sushiswap and Uniswap is liquidity rewards. In Uniswap, those who provide more liquidity receive more trading fees, leading to smaller liquidity providers becoming diluted as the LPs grow. Conversely, early adopters Sushiswap received 10x the amount of SUSHI as those who joined later, which could be used to receive trading fees from all pools even if the early adopters stopped providing liquidity. Moreover, when traders use SushiSwap, a portion of their fees are paid as dividends to token holders, bolstering the community and increasing the circulation and value of SUSHI. As such, the liquidity rewards provided in the form of SUSHI seek to create an incentive structure that encourages the adoption of Sushiswap pools, thereby leading to a positive feedback loop of increasing liquidity and volume.

Although the simple constant product invariant may seem less efficient than the newer, more robust models created by competing DEXs, Sushiswap's AMM is mathematically intuitive to traders and easy to use. The simplicity of the market making mechanism makes it much easier to compute swaps, leading to lower transaction costs for users. In addition, Sushiswap's more approachable system increases its decentralization, as they do not need raise funds for development from third-party organizations and can instead completely rely on the community.

4.1.2 UniswapV3

Uniswap, one of the first decentralized exchanges to use the constant product invariant recently released Uniswap V3, which allows liquidity miners to set price limits for their tokens. Uniswap V3 Liquidity pools contain a set of positions, each characterized by its liquidity and price limits, defined by L and $[p_a, p_b]$ respectively. Each of these positions, also known as ticks, abides by $(x+\frac{L}{p_b})(y+L\sqrt{p_a}) = L^2$; this formula makes it so that when a price limit is reached, real reserves (x or y) are exhausted, and the AMM moves on to the next tick. This system computes the constant product formula with virtual reserves, allowing for pricing to reflect that of AMM while making tokens added by miners only tradeable in a custom-set range.

Uniswap's concentrated liquidity model presents the advantage of greater capital efficiency and more virtual liquidity available for trading in the current price range. This leads to lower slippage and better swap execution for users. However, this comes with a tradeoff: the on chain implementation can also be more computationally intensive, especially on L1. In particular adding an LP position can cost upwards of 350,000 gas and swaps themselves cost a similar amount (gas usage varies based on swap), meaning that a singular transaction on Uniswap can potentially cost close to 0.03 ETH. Even with the Uniswap router, which designs routes for swaps to reduce gas cost, swapping on Uniswap remains more expensive than other DEXs.

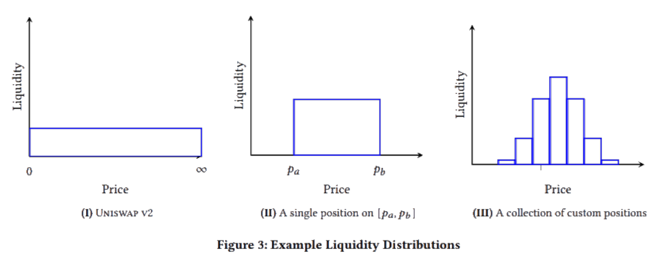

Fig. 2. Concentrated liquidity (Uniswap V3 Whitepaper)

Uniswap V3 also introduces a competitive landscape for liquidity providing. In many other DEXs as well as Uniswap V2, LPing was compartively uncompetitive, as liquidity provided by LPs would span the total range of prices for an asset pair, thus yielding some guaranteed fees from the pool. However, in Uniswap v3 the option to provide capital in specific price ranges allows for smarter actors to get a greater percentage of a pool's collected fees. On the other hand however, LP's who's liquidity falls outside the current price receive no share of the collected fees, thus exposing them to the risks of impermament loss and the volatility of the asset pair with no return. Overall, Uniswap's model creates a sizable advantage in terms of slippage and tradable liquidity compared to the simple constant product invariant implemented by Uniswap V2 and Sushiswap;

4.1.3 PancakeSwap V2

PancakeSwap V2 is one of the many Uniswap forks. Pancake Swap is a AMM DEX that is built on the Binance Smart Chain (a smart contract platform built by Binance) instead of Ethereum, which differentiates it from other Uniswap forks and AMM competitors. Pancake Swap also uses the BEP-20 Binance token standard instead of ERC-20, further separating it from competitors. Traders can use tokens from other platforms by wrapping them as a BEP-20 token via Binance Bridge. A major reason for Pancake Swap's success on Binance is their use of the Binance Exchange, which owns a huge store of the BNB tokens that are needed to vote for its 21 network-controlling nodes.

PancakeSwap ensures enough liquidity in the LPs by providing liquidity tokens for liquidity providers, which can later be used to collect trading fees and allowing for yield farming, a feature not offered by uniswap. By offering yield farming in such a way that balances our impermanent loss, Pancake Swap was able to gain huge traction after release as many traders moved their tokens from uniswap to Pancake swap to take advantage of this new feature. For traders, PancakeSwap's liquidity pools and staking options provide high appeal, as letting your tokens be locked up for a while can yield high interest. Pancake Swap also offers a host of gamified experiences that keep traders using their CAKE token, such as an NFT marketplace.

Since PancakeSwap smart constracts are deployed on Binance smart chain as opposed to the relatively more common Ethereum, this means that it comes with the benefit of faster gas fees and processes more transactions. However, Binance also runs a centralized exchange while not operating PancakeSwap allowing it to persist as a DEX. The Binance Smart has a delegated proof of stake consensus mechanism based on a set of validators. This generally implies (and practically results in) cheaper swap and contract interaction costs on Pancake swaps as opposed to Uniswap on Ethereum. This makes the liquidity more accessible and reduces capital barriers and efficiency limitations that prevents more retail users from accessing the Pancake DEX.

4.1.4 dYdX

Although dYdX is harder to compare against our other choices, as it's exchange mechanism is based on an order book it offers intriguing diversity in the space with its own architectural advantages. In fact, this approach using off-chain order books with on-chain settlement allows creation of efficient markets. As argued by the authors, this allows market makers to sign and transmit orders on an off-blockchain platform, with the blockchain only used for settlement. However, the AMM model replaces the order book with a system in which an asset's spot-price objectively responds to market forces and market participants on either side of the market trade with the AMM rather than with each other. This more standard alternative results in benefits such as availability (possibly at a worse price though) and smart contract integration.

Overall, dYdX is a margin trading platform based on Ethereum which allows borrowing, lending and speculation on the future prices of currencies. Options and derivatives mostly exist only in fiat / centralized exchanges, and this is precisely the problem dYdX aims to solve by transferring these financial products into the trustless / decentralized world. From a trader's perspective dYdX is rather limited in its choice of currencies (ETH, USDC, DAI) and two kinds of margin trading tools available: isolated and cross margin trading. However, lending here is relatively low-risk with interest earned every time a block is mined. Additionally, everyone is involved in one "global lending pool." There is no need to wait for capital sufficiency as each asset's pool is moderated by smart contracts.

Also, dYdX has a wide array of perpetual order types each with their own advantages and limitations. The extent of control of factors such as max slippage and good til date is considerable and contributes to diminishing the risk of operating on this platform. Furthermore, the recently added "trailing stop loss" feature is a concrete safety net for traders as it offers a way to update the stop price based on a "trailing percent." These dynamic control features (along with much more traditional financial instruments) make this a quite robust system and probably quite durable in the future.

4.1.5 Curve

Curve is a decentralized exchange known for its low slippage and low fees. The Curve StableSwap AMM emphasizes the exchange of similarly-priced stable coins, resulting in relatively low price variability, slippage, and impermanent loss (which is accounted for by fees, which are also low). StableSwap combines the linear invariant and constant product invariant via the following model, where N is the number of tokens in the pool, D is the sum invariant (i.e. $x+y+\ldots=D$), and A is the amplification coefficient. The amplification coefficient has the following effect: when the pool is unbalanced, the x-y curve (in the scenario when we have 2 coins) looks like the Uniswap curve ($xy=C$), and when the pool is balanced, the curve becomes more linear. Because of this, the formula strikes a balance between the lack of slippage accounted for in the linear invariance model, and the very high cost of rebalancing the pool in Uniswap. The following equation captures the AMM described above: $An^n\sum(x_i)+D=ADN^N+\frac{D^{N+1}}{N^N\prod(x_i)}$

The CurveCrypto invariant is a modification of StableSwap, allowing the exchange of relatively differently priced coins. The curve is more asymptotic, while still adhering closely to the modest linearity offered by StableSwap and the basic linear invariant. The additional asymptotic behavior deals with large variability in prices between differently priced assets (like the original Uniswap curve). A repegging algorithm is also used to adjust price ranges for coins, and this is all accomplished internally via an oracle, contrary to Uniswap. The following equation captures the AMM described above: $KD^{N-1}\sum x_i+\prod x_i=KD^N+(\frac{D}{N})^N$, where $K_0=\frac{N^N\prod(x_i)}{D^N}$ and $K=AK_0\frac{\gamma^2}{(\gamma+1-K_0)^2}$. γ is a positive number chosen to be small. Curve's combination of the constant product invariant and the constant sum invariant lead to lower slippage for traders.

In addition, to its low-slippage AMM design, Curve seeks to increase its usage through an effective incentive structure. The coins which are deposited into Curve gain interest because they are harnessed to supply other liquidity pools. This is done in addition to compensation for liquidity providers in the form of fees when an exchange is made on Curve. Curve incentivizes depositing coins which are in low amount in the pool (relative to the "balance point") via "deposit bonuses," increasing liquidity and volume as a result. Because coins in low quantity and more expensive, Curve's instantaneous deposit bonus has a large impact on Curve liquidity pools. Moreover, corporations often incentivize pools on Curve via bonuses, which can increase pool liquidity. Similar to Sushiswap, Curve seeks to reward users with its own cryptocurrency, and CRV tokens are being given to Curve participants. Another important point to note about Curve is that when a stable coin is exchanged, that coin is split into all the coins in the pool, allowing for diversification, which can also benefit liquidity providers. However, the complexity of Curve's structure is not without its downsides. Because Curve's smart contracts rely on the smart contracts of other pools, risk is additive.

4.2 Relevant Visualisations

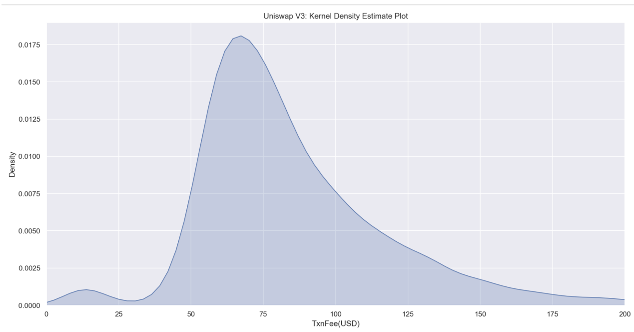

Fig. 3. Uniswap Transaction Fees

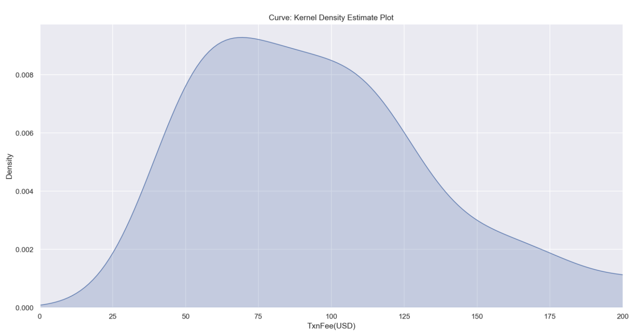

Fig. 4. Curve Transaction Fees

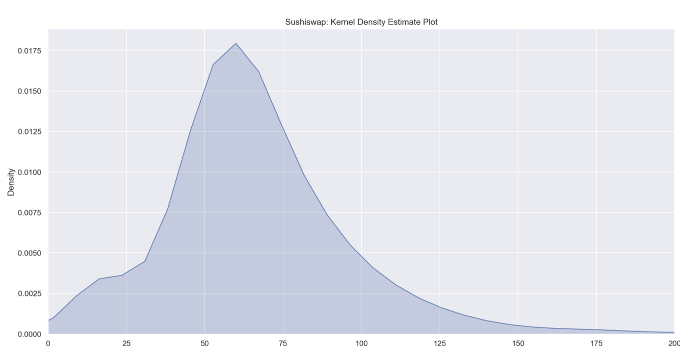

Fig. 5. SushiSwap Transaction Fees

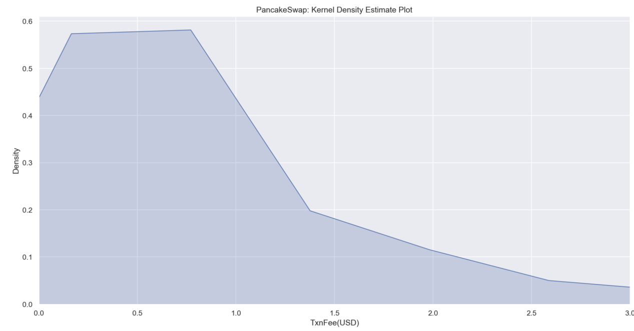

Fig. 6. Pancake Swap Transaction Fees

4.3 System Design and Implementation

In this section, we propose a system that could potentially be used to optimize execution of cryptocurrency swaps by performing swaps in multiple exchanges. In doing so, we can seek to provide insight on the underlying reasons for the success of these exchanges over others, and formalize the theory driving popular DEX aggregators like 1inch. The optimization proceeds as follows. Each DEX possesses a Model in the system design. Each model takes in parameters featured in that DEX's Automated Market Maker's equation. Each model also features a function which calculates how much of token Y we would receive when selling an amount of token X. These functions take the amount of Token X as input. It is important to note that the updated parameters for the AMM are found using API calls to the appropriate DEX interfaces. Then we formulate an optimization problem which poses the following general question: if we want to attain a return of a input amount of Y, what is the minimum amount of X we can sell (across the 3 exchanges we consider)? To do this, we perform minimization under the following constraints:

$$\min \sum_{i=1}^{N} X_i$$

$$\forall X_i \geq 0 \quad \sum_{i=1}^{N} Ret_{DEX_i}(X_i) = amount_Y$$

X_i represents the amount of X we sell in exchange i.
In particular, we build Python models for the following exchanges: Curve v2, Uniswap v3, Sushiswap. It is important to note that dYdX is not included due to its order book philosophy, while the aforementioned exchanges utilize AMMs. Indeed, it is the formulaic nature of these AMMs which allows us to frame our situation as a mathematical optimization problem. Models in python are represented via classes, each with a specific instance function which returns the amount of Y out given an amount of X in.

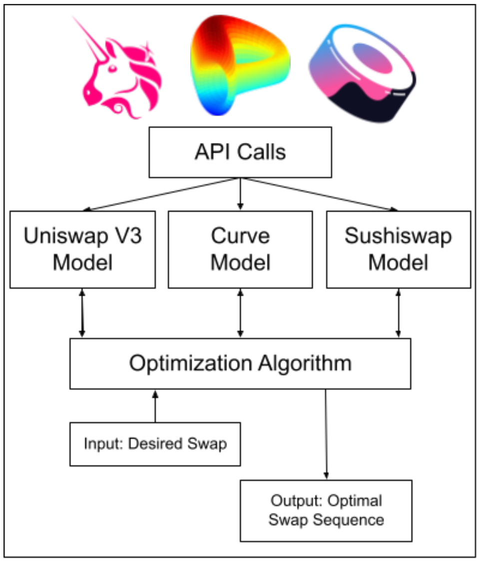

Fig. 7. Cryptocurrency Swap Recommendation System

We then use Scipy's *minimize* function to perform the optimization to minimize $X_1 + X_2 + X_3$. We use the method of Sequential Quadratic Programming (SLSQP) (although a method like gradient descent would also be fine and the methods are interchangeable) to find the minimum of the non-linear program. SLSQP minimizes iteratively, only harnessing "active" constraints at a given time-step.
The Python code we wrote for this system is available at: https://github.com/huhabu/DefiProjectOptimization

5. Conclusion

As the global market continues to adopt blockchain and cryptocurrency, the need for decentralized exchanges will continue expand. In this paper, we outline a breadth of market making mechanisms used by the most popular decentralized exchanges. Beyond the the unifying factor of decentralization, each respective exchange explored in this paper has unique attributes designed to maximize the efficiency of swapping, as well as attracting liquidity providers to add to liquidity pools. The wide array of computational and business models employed by these exchanges present varying advantages, making them optimal for different traders and providers. Overall, we think that our analysis actually argues for the importance of having a range of options rather than a mono/duopoly by illustrating the unique advantages and limitations each of these protocols offer.

BIBLIOGRAPHY

[1] UNISWAP v3 core. (n.d.). Retrieved November 1, 2021, from https://uniswap.org/whitepaper-v3.pdf.

[2] Guillermo Angeris and Tarun Chitra. 2020. Improved Price Oracles: Constant Function Market Makers. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (AFT '20). Association for Computing Machinery, New York, NY, United States, 80–91. https://doi.org/10.1145/3419614.3423251

[3] Michael Egorov. 2019. StableSwap - Efficient Mechanism for Stablecoin Liquidity. Retrieved Feb 24, 2021 from https://www.curve.fi/stableswap-paper.pdf

[4] Allan Niemerg, Dan Robinson, and Lev Livnev. 2020. YieldSpace: An Automated Liquidity Provider for Fixed Yield Tokens. Retrieved Feb 24, 2021 from https://yield.is/YieldSpace.pdf

[5] Abraham Othman. 2012. Automated Market Making: Theory and Practice. Ph.D. Dissertation. Carnegie Mellon University

[6] Antonio Juliano. 2018. A Standard for Decentralized Margin Trading and Derivatives. Retrieved Nov 1, 2021 from https://whitepaper.dydx.exchange

[7] Matt Hussey, K. C. T. (2020, April 27). What is dydx? A 3-minute guide to the Margin Trading Platform. Decrypt. Retrieved November 1, 2021, from https://decrypt.co/resources/dydx-ethereum-margin-trading-platform-explained-learn.

[8] Perpetual order types. dYdX Help Center. (n.d.). Retrieved November 1, 2021, from https://help.dydx.exchange/en/articles/4797992-perpetual-order-types.

[9] What is Sushi? Sushi. (n.d.). Retrieved November 1, 2021, from https://docs.sushi.com/.

[10] Dale, B. (2021, May 28). Liquidity mining will return to Uniswap 'very soon,' founder says. CoinDesk Latest Headlines RSS. Retrieved November 1, 2021, from https://www.coindesk.com/markets/2021/05/28/liquidity-mining-will-return-to-uniswap-very-soon-founder-says/.

[11] PancakeSwap. (n.d.). Retrieved November 1, 2021, from https://docs.pancakeswap.finance/.

[12] Curve StableSwap: A comprehensive mathematical guide. Xord. (2021, October 7). Retrieved December 14, 2021, from https://xord.com/research/curve-stableswap-a-comprehensive-mathematical-guide/.

[13] Ask any difference. Ask Any Difference. (2021, August 5). Retrieved November 1, 2021, from

https://askanydifference.com/difference-between-pancakeswap-and-uniswap/PancakeSwa-vs-Uniswap.

[14] Sok: Decentralized exchanges (DEX) with automated ... - arxiv. (n.d.). Retrieved November 1, 2021, from https://arxiv.org/pdf/2103.12732.pdf.

[15] Automatic Market-Making with Dynamic PEG - Curve.fi. https://curve.fi/files/crypto-pools-paper.pdf.

[16] "What Is Curve.fi?" Understanding Curve - Curve Finance, https://resources.curve.fi/base-features/understanding-curve.

[17] Lindsay X. Lin, L. C. at I. and S. D. F. (2019, January 5). Deconstructing decentralized exchanges · Stanford Journal of Blockchain Law Policy. Stanford Journal of Blockchain Law Policy. Retrieved November 1, 2021, from https://stanford-jblp.pubpub.org/pub/deconstructing-dex/release/1.

[18] Capponi, A., Jia, R. (2021, July 21). The Adoption of Blockchain-based Decentralized Exchanges. Retrieved November 1, 2021, from https://arxiv.org/pdf/2103.08842.pdf.

[19] Curve.fi. https://curve.fi/stableswap-paper.pdf.

[20] Powers, Chris. "Curve V2 Takes on UNISWAP, BTC on Ethereum Grows." Dose of DeFi, Dose of DeFi, 10 June 2021, https://doseofdefi.substack.com/p/curve-v2-takes-on-uniswap-btc-on.

[21] Curve Market Cap. "June 9, 2021: Curve V2 Live." Curve Market Cap, Curve Market Cap, 9 June 2021, https://curve.substack.com/p/june-9-2021-curve-v2-live?r=br6usamp;utm-campaign=twitter.

[22] 0X White Paper - 0X: Powering the decentralized exchange ... (n.d.). Retrieved December 14, 2021, from https://0x.org/pdfs/0x$_{w}hite_{p}aper.pdf$.