IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Special Issue 2, April 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

Automated Market Makers an Efficient AMM Algorithm for Low Slippage of Traded Assets

Albin. A

U.G. Student, Department of CSE, Velammal Engineering College, Chennai, Tamil Nadu, India

ABSTRACT: Automated Market Makers (AMMs) are a popular decentralised finance (DeFi) application that enables users to trade different types of crypto-tokens without the need for intermediaries. There are various implementations and models of AMMs, each featuring sophisticated economic mechanisms. In this paper, we present a theoretical framework for AMMs that provides a formal proof of their fundamental properties, encompassing both structural and economic aspects. The proposed theory performs better than existing systems by delivering low slippage transactions. Slippage is the difference between the price we are proposed by the algorithm before the transaction takes place and the actual price the transaction gets filled. By abstracting from the actual mechanisms and focusing on the necessary conditions, we prove the validity of our theory. We solve the arbitrage problem, which is the main game-theoretic foundation behind AMMs' economic mechanisms. Overall, the proposed AMM offers a practical solution to the limitations of current AMMs over binary events and has the potential to improve liquidity and profitability in decentralised exchanges.

KEYWORDS: Automated Market Makers, Decentralized Exchanges, Blockchain, Liquidity Pools, Trading Pair, Exchange Rates, Transparency, Efficiency.

I. INTRODUCTION

Decentralized finance (DeFi) is a rapidly growing field in the world of blockchain technology, offering an alternative to traditional finance by allowing users to create and trade crypto-tokens without intermediation from central authorities. One of the main archetypes of DeFi is Automated Market Makers (AMMs), which are decentralized markets of crypto-tokens that offer users three core operations: depositing crypto-tokens to obtain shares in an AMM, redeeming shares in the AMM for the underlying tokens, and swapping tokens of a given type for tokens of another type.
Although AMMs may appear straightforward, they exhibit an emerging behaviour where users are incentivized to swap tokens to keep their swap rates aligned with the exchange rate, which is the ratio between the prices of the exchanged tokens given by external price oracles. Interactions with AMMs are sensitive to transaction ordering attacks, where actors with the power to influence the order of transactions in the blockchain can profit from opportunistic behaviour, causing detriment to other users.

Primarily there are 2 types of market makers, The traditional one being an Order Book market, Where each order requires 2 entities taking part in the transaction (Seller and Buyer). The other type is an Automated Market Maker, Where there is a pool of assets called the Liquidity Pool that is used by an algorithm to fill orders. The price of the order is determined by the ratios of the assets in the liquidity pool and the order is satisfied instantly without needing another party to fill an order. AMMs are still in their primitive stages facing problems which prevent it from being mass adopted.

To address these challenges, there is a need for foundational work to devise formal theories of AMMs that allow for an understanding of their structural properties and economic incentive mechanisms. Current descriptions of AMMs are either economic models or concrete AMM implementations. Economic models are useful to understand the macroscopic financial aspects of AMMs, but they do not precisely describe the interactions between AMMs and their users. On the other hand, implementations reflect the exact behaviour of AMMs, but at a level of detail that hampers high-level understanding and reasoning. Moreover, the rich variety of implementations, proposals, and

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

models for AMMs, each featuring different economic mechanisms, makes it difficult to compare AMM designs or provide a clear contour for the space of possible "well-behaving" designs.

Therefore, a more precise formalization of AMMs' interactions with their users is fundamental to understand the structural and economic properties of AMMs and to determine possible deviations from safe behaviour. The project aims to fill this gap by providing a platform for high-quality research on AMMs, including the development of new economic models and formal analyses of AMM implementations.

II. IMPORTANT TERMS

Assets: Tokens in a DEX refer to digital assets that are traded on a decentralized exchange. Tokens can be cryptocurrencies, stablecoins, or other assets, each represented by a unique digital token created and managed on a blockchain. DEXs allow users to trade these tokens without relying on a centralized intermediary, using smart contractsto facilitate peer-to-peer trading.

Liquidity Pools: Liquidity pools are a DeFi mechanism that enables users to provide liquidity for a cryptocurrency or token. They are a pool of funds locked in a smart contract and used to facilitate trades on a DEX without affecting the price of the underlying asset. Users deposit their cryptocurrency into a liquidity pool and receive LP tokens representing their share of the pool. When a trade is made, the smart contract executes it using the funds in the pool, acting as a market maker. Liquidity providers earn a share of the trading fees generated by the pool in proportion to their share of the pool. Liquidity pools are an innovative solution to the problem of liquidity in cryptocurrency markets, providing a decentralized mechanism for facilitating trades and allowing users to earn a passive income by providing liquidity to the pool.

Reserves: Token reserves in liquidity pools refer to the amount of a particular cryptocurrency or token held in the pool. These reserves are used to facilitate trades on a DEX and earn liquidity providers a share of the trading fees generated by the pool.

Asset Price: Asset price is determined by the supply and demand of the token in the liquidity pool. When there is more demand for a token, the price increases, and when there is less demand, the price decreases. This automated market-making system uses algorithms to adjust the price based on trading activity, ensuring that the price is always reflective of the market conditions.
The formula is x * y = k, where x and y represent the reserves of the two tokens in a liquidity pool, and k is a constant value. This formula ensures that the product of the two token reserves remains constant, even as the price changes due to supply and demand. The formula is used to calculate the exchange rate for trades on the platform, ensuring that usersreceive a fair price for their trades based on the current market conditions.

Quote Amount: Quote amount refers to the amount of cryptocurrency or token that a user is willing to trade for another. This quote amount, along with the current market price, is used to calculate the exchange rate for the trade. When a user submits a trade order, the quote amount is locked in a smart contract until the trade is executed. The quote amount ensures that users receive a fair exchange rate for their trades on a DEX.

Slippage: Slippage refers to the difference between the expected price of a trade and the actual price at which the trade is executed. It occurs due to the dynamic nature of liquidity pools, where the price of a token can change based on the amount of liquidity available in the pool. If a user places a large order that exceeds the available liquidity in the pool, the trade will be executed at a higher price, resulting in slippage. To mitigate this risk, DEXs often display slippage information to users and allow them to adjust their quote amount to ensure they receive a fair exchange rate.

It is the difference between the expected and realized price of a trade. Unlike traditional exchanges that match buy and sell orders, AMMs determine exchange rates on a continuous curve, resulting in slippage that is dependent on trade size, pool size, and conservation function design. While spot price approaches realized price for small trades, it deviatesmore for larger trades, particularly in smaller liquidity pools. Continuous slippage requires trades on AMMs to be set with slippage tolerance for execution, which can be exploited for sandwich attacks.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

III. METHODOLOGY

Users can trade cryptocurrencies using Automated Market Makers (AMMs), a type of decentralized exchange (DEX), without utilizing a conventional order book or centralized exchange. Instead, AMMs use smart contracts and mathematical algorithms to determine asset prices and carry out trades automatically.

The fundamental goal of AMMs is to establish a liquidity pool against which customers can engage in trading. Users who deposit equal amounts of various tokens with different values into a smart contract can create liquidity pools, which are made up of two or more tokens. The price of each token in relation to the others is then determined by a mathematical formula in the smart contract that controls the pool. The "constant product" formula, which guarantees that the product of the quantities of two tokens in a pool remains constant as users trade those tokens, is typically used for this.

AMMs are designed with the goal of creating a pool of assets that can be traded. For instance, users would contributeequal amounts of ETH and USDC to the pool in a straightforward AMM for trading Ethereum (ETH) and a stablecoin like USDC. The price of each token would then be determined by the AMM's smart contract based on the relative proportions of each token in the pool. The equation x*y=k, where x represents the amount of ETH in the pool, y represents the amount of USDC in the pool, and k represents a constant value, referred to as the "constant product" formula.

Users only need to exchange tokens at the current price established by the AMM algorithm when they want to buy orsell a token. As an illustration, if a user wants to purchase ETH with USDC, they would send USDC to the AMM and receive ETH at the going rate in return. The smart contract then modifies the pool size and cost in accordance with the constant product equation.

The fact that AMMs are permissionless, allowing anyone to trade without the use of middlemen, is one of their main benefits. As the smart contract is always active and capable of carrying out trades automatically, this enables trading at any time. As long as there are enough liquidity providers eager to contribute assets to the pool, AMMs can also be usedto trade illiquid assets that might not have enough trading volume to be listed on centralized exchanges.

Due to their accessibility, transparency, and automation of trading processes, AMMs are a well-liked DeFi application. AMMs are likely to become more crucial to the decentralized economy as bitcoin and DeFi continue to advance.

III. EXISTING MODEL & PROPOSED SOLUTION

The solution to trade correlated assets with better prices is to make them fit a tighter price curve. The existing curve is given by the equation x*y = K, Where x and y are the liquidity pool sizes of the 2 respective tokens. This is a broad price curve which is very advantageous for non correlated assets and allows for sudden drastic price changes.

For the perfect prices, the tokens should have the same value even after multiple buys and sells. So Price(x) = Price(y). Essentially the amount of tokens in each pool should amount to a constant always, This is denoted by x+y = K, Only issue with this curve is it can completely drain the liquidity pool and that is not favourable.

A viable solution price curve should follow the x+y = K line when there is liquidity and the x*y = K curve when there is less liquidity to prevent the pool from draining out. Therefore we must combine the line x+y = k and curve x*y = k toobtain a more efficient price curve.

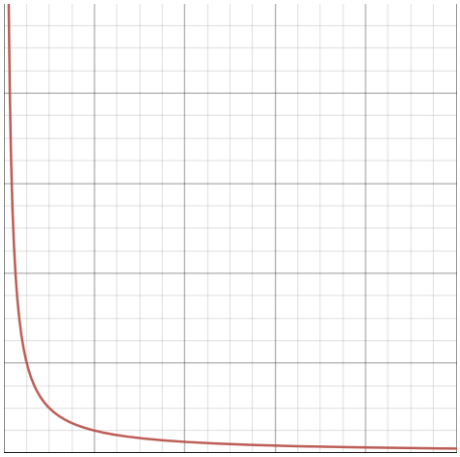
By combining the circle which has x+y = K as tangent and the hyperbola x*y = k with x and y axes as its asymptotes we get the curve x^3 * y + y^3 * x = k, The price curves for are shown in the graph below

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India



*Fig, 1.1: x*y = K curve*

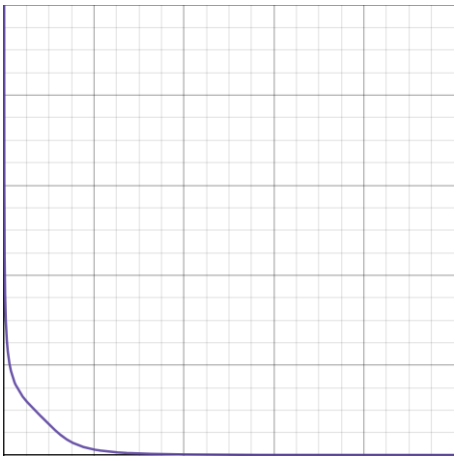


*Fig 1.2: x^3 * y + y^3 * x = k*

As we can see, The latter graph has a tighter price curve and hence provides a better price for correlated assets.

IV. EXPERIMENTAL RESULTS

Fig 2.1: Transaction with old curve

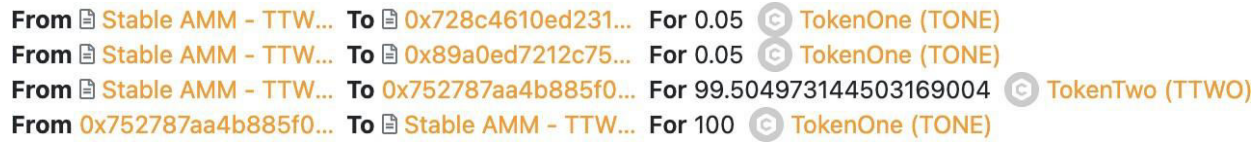


Fig 2.2: Transaction with new curve

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

We can evidently see that for a correlated asset with 1:1 value, For the same transaction amount, The old curve gives out 88 tokens, Whereas the new curve gives out 99.5 tokens. This is a drastic improvement in price and slippage.

V. RELATED WORK

Zohar et al. (2021) propose a mechanism called atomic arbitrage, which prevents front-running by ensuring that all trades are executed atomically. Li et al. (2021) propose a solution called LiME, which uses a commitment scheme to prevent sandwich attacks.AMMs and DEXs are vulnerable to various types of attacks, including front-running, sandwich attacks, and liquidity pool draining.Liquidity pool draining attacks occur when a malicious actor withdraws liquidity from a pool by exploiting the AMM's pricing algorithm. Many works have focused on analyzing these attacks and proposing countermeasures

Golovin et al. (2021) propose a model called Optimal Swap Pricing (OSP), which optimizes the swap rate to minimize slippage and gas costs. Similarly, Wang et al. (2021) propose an optimization framework called Optimized Automated Market Makers (OAMMs), which considers both the accuracy and the computational cost of the AMM's pricing algorithm.AMMs are subject to a trade-off between accuracy and efficiency. A more accurate pricing algorithm may result in a better price for the user, but it may also require more computational resources and result in higher gas fees.

Aspnes et al. (2021) propose a mechanism called SafeSwap, which incentivizes liquidity providers to stay in the market by rewarding them for holding on to their shares for a longer time.AMMs rely on liquidity providers to provide liquidity to the market, and the depth of the market is a critical factor in determining the effectiveness of an AMM.

Many works have focused on analyzing the liquidity and market depth of AMMs and proposing methods to increase liquidity.

VI. CONCLUSION

In conclusion, this paper has presented a comprehensive overview of Automated Market Makers (AMMs) and their use in decentralized exchanges (DEXs) within the DeFi space .We present a new liquidity-sensitive market maker design that overcomes these challenges while retaining path independence, ensuring that the market maker cannot be exploited and simplifying implementation. Our design relaxes the arbitrage condition that constrains prices of disjoint and exhaustive assets to sum to exactly one dollar, enabling prices to sum to more than one. This practical benefit allows the market maker to extract a profit if the entropy of final prices is sufficiently high.
This proves that if we want sensitivity for liquidity and path independence, then we must relax the arbitrage condition. Additionally, demonstration of liquidity-sensitive market maker requires a lower subsidy to achieve reasonable liquidity than LMSR, and it actually makes a profit for a broad range of terminal market states, regardless of the event that gets realized.

In conclusion, our liquidity-insensitive market maker design with new price curves offers a practical solution to the challenges faced by existing AMM designs, providing liquidity insensitivity while retaining path independence.

REFERENCES

[1] "An Overview of Decentralized Exchanges (DEXes)" by Karteek Kotamraju and Sethuraman Subbiah (2019)
[2] "AMM DEX for Near-Instantaneous Settlement and Feeless Transactions on Blockchains" by Samiran Roy, Yashar Ghiassi-Farrokhfal, and Ashraf Abdel-Kafi (2021)
[3] "A Survey on Automated Market Makers in Blockchain-Based Decentralized Finance" by Muhammad Salman Khan, Muhammad Aamir Cheema, and Athanasios V. Vasilakos (2021)
[4] "Liquidity Sharing in Decentralized Exchanges: Challenges and Opportunities" by Xinyi Yang, Zhouxiang

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

Shen, and Shengwu Xiong (2021)

[5] “A survey of blockchain technologies for open innovation: platforms and applications" by Vigneswaren Arunachalam, Vinoth Kumar Selvam, and Jeng-Fung Chen (2021)

[6] "A Novel Approach to Liquidity Provision in Decentralized Exchanges," by William J. Knottenbelt, Maria Apostolaki, and Christian J. Goguen. IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), 2018.

[7] "Liquidity Provision in Decentralized Exchange Protocols," by Aditya Asgaonkar, Varun Murali, and Vivek Bindiganavale. IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), 2018.

[8] "Real-Time Exchange Rate Calculation and Arbitrage Detection with Blockchain Technology" by Sebastian Fuhrhop, Sebastian Gebhard, Philipp Sandner, and Matthias Reumann, published in the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).

[9] "A Blockchain-Based Dynamic Currency Exchange System with Liquidity Management" by Armando Walter Colombo and Marco Di Benedetto, published in the 2020 IEEE Access journal.

[10] "Uniswap: A Protocol for Decentralized Exchange on Ethereum" by Hayden Adams (2018)

[11] "Automated Market Making with Non-Convex Trading Fees" by Bowen Liu et al. (2021)

INNO SPACE
SJIF Scientific Journal Impact Factor

SJIF: 8.423

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details