American International University-Bangladesh (AIUB)

Thesis

Mitigation of Front Running Attack in DeFi by Optimizing Automated Market Makers (AMMs) Algorithm

Submitted By

Name	ID
TAMIMUL ALAM	**20-42215-1**
MD. RABBI ISLAM SAJID	**20-42181-1**
MD. HASIBUR RAHMAN	**20-42180-1**
MD. MUSTAFIZUR RAHMAN	**20-43584-1**

This Thesis submitted for the degree of Bachelor of Science

(BSc) in Computer Science and Engineering (CSE) at

American International University Bangladesh in June, 2023

Faculty of Science and Technology (FST)

Author Declaration

We declare that this project is our original work. No part of this has been submitted elsewhere partially or fully for the award of any other degree. Any material reproduced in this project has been properly acknowledged.

We declare that this project does not contain any content that discloses the secret of any organization or related parties. American International University-Bangladesh (AIUB) will not be held liable for any such activity, as the project is presented as our original work.

_____
TAMIMUL ALAM
20-42215-1
Department: CSE

_____
MD. RABBI ISLAM SAJID
20-42181-1
Department: CSE

_____
MD. HASIBUR RAHMAN
20-42180-1
Department: CSE

_____
MD. MOSTAFIZUR RAHMAN
20-43584-1
Department: CSE

Approval

The thesis titled Mitigation of Front Running Attack in DeFi by Optimizing Automated Market Makers (AMMs) Algorithm has been submitted to the following respected members of the board of examiners of the department of computer science in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science on 8 June, 2023 and has been accepted as satisfactory.

Prof. Dr. Md. Asraf Ali
Supervisor
Department of Computer Science
American International University-Bangladesh

Dr. Md. Mehedi Hasan
External
Department of Computer Science
American International University-Bangladesh

Dr. Akinul Islam Jony
Head [Under Graduate Program]
Department of Computer Science
American International University-Bangladesh

Prof. Dr. Dip Nandi
Associate Dean
Faculty of Science and Technology
American International University-Bangladesh

Mashiour Rahman
Sr. Associate Professor & Dean-in-charge
Faculty of Science and Technology
American International University-Bangladesh

Acknowledgment

First and foremost, we express our deepest gratitude to the Almighty Allah for His abundant blessings. With His divine guidance, we have completed our thesis. We are truly grateful for the smooth progression of our work without any significant setbacks.

We extend our sincere appreciation to our supervisor, Prof. Dr. Md. Asraf Ali, for his invaluable support, guidance, advice, and encouragement throughout our thesis. His unwavering willingness to assist us whenever we needed it has been instrumental in our success.

Lastly, we are deeply indebted to our parents for their unwavering support. Their kind assistance and fervent prayers have played a crucial role in our journey, and we acknowledge that without their constant encouragement, we may not have been able to achieve our goals. We are now on the threshold of graduation, and we attribute a large part of our accomplishments to their love and guidance.

TABLE OF CONTENTS

Author Declaration 2
Approval 3
Acknowledgment 4
TABLE OF CONTENTS 5
LIST OF TABLES 7
LIST OF FIGURES 8
LIST OF ABBREVIATIONS 9
Abstract 10
CHAPTER 1: INTRODUCTION 11
1.1 Background 11
1.2 Motivation of the Research 12
1.3 Problem Statement 14
1.4 Research Questions 16
1.5 Research Objectives 17
1.6 Research Scope 17
CHAPTER 2: LITERATURE REVIEW 18
2.1 DeFi Security Issues 18
2.2 Front-running attack in DeFi 19
2.3 Uniswap v3 20
CHAPTER 3: RESEARCH METHODOLOGY 21
3.1 Article Collection Method 21
3.2 Liquidity Concentration 31
3.3 Mathematical Approach 36
CHAPTER 4: RESULTS AND DISCUSSION 43
4.1 Efficient Techniques 43
4.2 Automated Market Makers (AMMs) Algorithm 44
4.3 Results and Findings 46
CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS 50
5.1 Findings and Contributions 50

5.2 Recommendations for Future Works 51
REFERENCES 52
APPENDIX 59

LIST OF TABLES

Table 3.1: Key Data 21

LIST OF FIGURES

Figure 1.1**:** The metaverse's development was divided into three distinct stages. 12
Figure 1.2**:** Decentralized Financial (DeFi) System. 13
Figure 1.3**:** Data is added to the blockchain for transactions..... 15
Figure 1.4**:** Example of Front Running in a Quiz game. 16
Figure 3.1**:** Article search results. 30
Figure 3.2**:** Control Flow Diagram of Liquidity Concentration Algorithm..... 34
Figure 4.1**:** Comparison of accuracy before and after the optimization. 47
Figure 4.2**:** Price slippage and accuracy improvement in graph plotting. 47

LIST OF ABBREVIATIONS

AMM = Automated Market Maker

ADF = Augmented Dickey-Fuller

ARDL = Autoregressive Distributed Lag

BCI = Blockchain Intelligence

CFMMs = Existing constant function market makers CFMMs

DeFi = Decentralized Finance

DFGLS = Dickey-Fuller GLS

DEXS = Decentralized Exchanges

ETH = Ethereum

GQL = Graph Query Language

LP = Liquidity Pool

MEV = Miner/Maximal Extractable Value

Mempool = Memory Pool

PP = Phillips-Perron

TOD = Transaction Ordering Dependence

VECM = Vector Error Correction Model

Abstract

The Metaverse, is a mirror of the physical world that is currently under development and promises to offer a new way of socializing, conducting business, and interacting with digital assets. This new technology will revolutionize all aspects of the physical world and its typical ecosystem. The typical financial structure of the world will be changed and completely converted into a decentralized finance technology which is called Decentralized Finance (DeFi). Decentralization finance (DeFi) will replace the typical financial ecosystem and provide more secure asset transactions based on Blockchain technology. Though decentralization could provide a risk-free and efficient solution for the total financial ecosystem in Metaverse, it has some issues that should be recognized. The potential security risks are the main concern before completely diving into the whole financial decentralization process. This paper highlights the main role of DeFi in the Metaverse financial ecosystem as well as the DeFi security issues. Among the various types of security issues that have been raised over time in DeFi, one of the primary concerns is the Front running attack, which can result in significant financial losses for investors and can undermine the integrity of the Defi ecosystem. Finally, the paper will provide a probable solution to the Frontrunning attack of Decentralized Finance (DeFi) in the Metaverse financial ecosystem.

Keywords: Metaverse, DeFi, Blockchain technology, Front running

CHAPTER 1: INTRODUCTION

1.1 Background

Decentralized Finance (DeFi) is a rapidly growing area of the cryptocurrency industry that seeks to provide users with financial services that are more accessible, transparent, and secure than traditional finance [1]. At the same time, the Metaverse is an emerging concept that aims to create a fully immersive virtual world that can be accessed by anyone, anywhere at any time [2]. As these two areas are converging gradually, there is enormous potential for DeFi to provide risk-free and efficient financial services within the Metaverse.

The prefix "meta" (which means transcendence) and the suffix "verse" (short for the universe) were combined to form the term "metaverse," a virtual universe with a consistent moral code and a separate economic system connected to the real world [3]. A user can engage in a variety of virtual activities, from gaming and socializing to purchasing virtual goods and taking part in virtual economies, according to Neil Stephenson, who first used the term in his science fiction book Snow Crash in 1992 [4]. Users can enter the metaverse through digital avatars using virtual reality equipment. Since its inception, the idea of the metaverse has been described in a variety of ways, including as a second life [5], 3D virtual worlds [6], and life-logging [7]. The actual, natural, and digital worlds are combined in a completely immersive, highly spatiotemporal, and self-sustaining virtual shared place [8]. The metaverse incorporates several cutting-edge technologies, including digital twins, virtual reality, augmented reality, 5G, wearable sensors, BCI, artificial intelligence, and blockchain/NFT, which is crucial in determining the true ownership of content as well as the rights to metaverse assets [9]. The metaverse is soon to emerge from its infancy into an emerging

reality, drawing increasing interest from all around the world thanks to the popularity of smart gadgets and the maturation of enabling technologies. Numerous tech behemoths have announced their forays into the Metaverse, with Facebook changing its name to "Meta" to focus on creating the metaverse of the future [10].

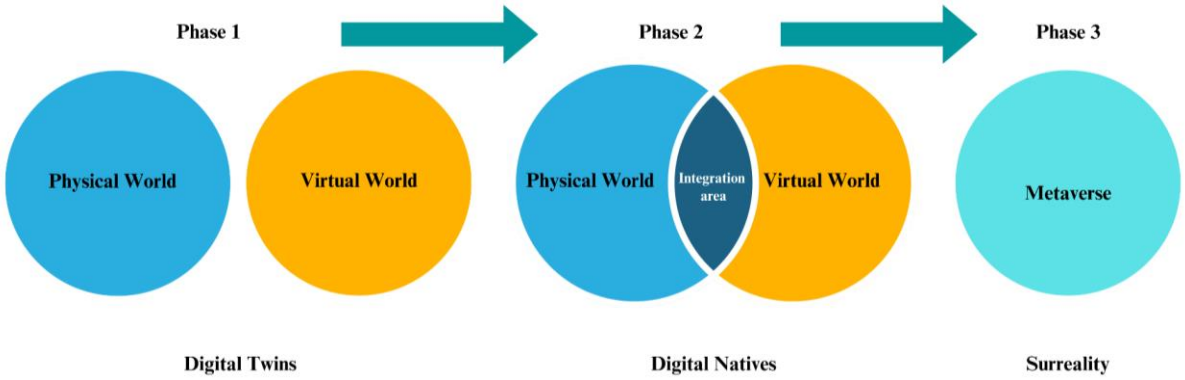

Figure 1.1**:** The metaverse's development was divided into three distinct stages.

1.2 Motivation of the Research

DeFi is a term used to describe financial services and products that are accessible to anyone with an internet connection and access to the Ethereum network [11]. DeFi's ability to provide open markets that are always accessible without allowing any central authorities to obstruct payments or restrict access is what makes it special. DeFi is a desirable option because it uses code to handle functions that were previously slow and subject to human error as well as to increase security [12].

Decentralized finance (DeFi) is a new and rapidly expanding field within the Bitcoin industry to improve financial inclusion by providing internet-connected people with access to financial services [13]. It is based on decentralized blockchain technology, particularly Ethereum, which enables peer-to-peer interactions between consumers and financial products and services without

the need for middlemen like banks or other financial institutions [14]. Oracles are used by several well-known DeFi protocols, including Compound, MakerDao, Uniswap, and Aave, to retrieve outside data. In these use cases, bitcoin exchange rate information is gathered by oracles and sent to requesting DeFi applications [15].

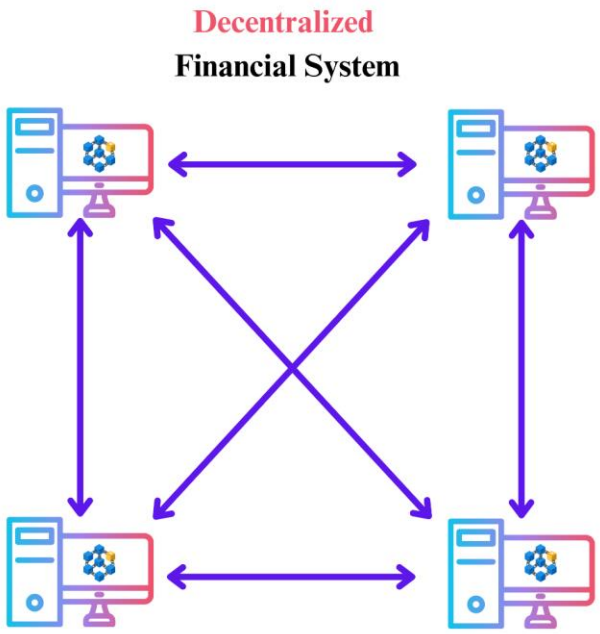

Figure 1.2**:** Decentralized Financial (DeFi) System.

One of the key benefits of DeFi is the open and accessible nature of its markets. Because there are no centralized authorities or gatekeepers, anyone can participate in the markets at any time, and payments cannot be blocked or restricted. Additionally, DeFi services are often faster and more reliable than traditional financial services, as they are automated and powered by code that can be easily audited and scrutinized by anyone [16].

Decentralized finance (DeFi) has emerged as a crucial component of the growing metaverse ecosystem [17]. DeFi refers to financial applications built on blockchain networks that operate in

a decentralized manner, without the need for intermediaries such as banks. DeFi enables users to access a range of financial services, such as lending, borrowing, trading, and earning interest, with greater transparency and control [18]. In the Metaverse, DeFi can provide a secure and transparent framework for conducting digital transactions. Overall, DeFi can enhance the user experience in the Metaverse by providing a secure and decentralized financial infrastructure.

DeFi can provide a transparent banking system but it is not risk-free [19]. Like any financial system, there are inherent risks involved in using DeFi protocols. One of the main risks of DeFi is Front running that can analyze smart contract instructions and functions theory that has never been used in a smart contract before to extract potential gains and cut off funds [20]. The aim is to provide an optimal solution to the Front running problem and how to mitigate the security risks that will arise in Decentralized Finance (Defi).

1.3 Problem Statement

Cryptocurrency exchanges today hold more than $10 billion in trade volume per day [21]. This is a whole new concept that creates a vast scope for the financial system to be fully transformed into a decentralized platform based on Blockchain technology. This new financial concept will be known as Decentralized Finance (DeFi). In DeFi technology a popular alternative for centralized asset-to-asset transactions is a decentralized exchange (or “DEX”) [22]. This decentralized exchange technology will exchange digital assets as NFTs in DeFi technology with the help of Blockchain ledgers. However, DeFi is not completely safe because attacks on it continue to happen occasionally [23]. One of the main security concerns that will create instability and disbelief from decentralized finance technology is a “Front running attack”. This front-running attack also known as a “Sandwich attack” will generate an advantage for an attacker who will take advantage of the

process by which transactions are uploaded to the blockchain's distributed ledger [24]. To dive into the Front running concept in DeFi, we need to understand some terms and how transactions are submitted to the blockchain to understand the vulnerability [25]. Therefore, a transaction is not immediately added to a block when the user submits it to the node. These unmined transactions are kept in a sort of waiting area called Mempool (a combination of "memory" and "pool") before being verified [26].

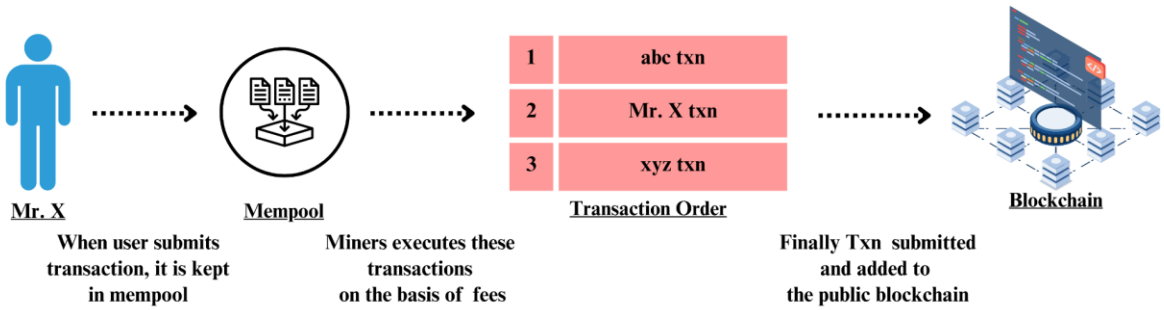

Figure 1.3**:** Data is added to the blockchain for transactions

The mempool is a storage area in a node where validated transactions wait to be added to the blockchain by miners [27]. Miners prioritize transactions based on fees, and transactions with higher fees are more likely to be included in the next block. Therefore, the higher the fees, the faster the transactions will be processed [28].

Front-running attacks exploit the way transactions are added to the blockchain. Malicious users watch transactions waiting in the mempool, then send their transactions to profit from higher gas prices [29]. This causes the attacker's transaction to be executed before the original user's transaction, as the miner or bot places the attacker's transaction in front of the pending one [30].

For instance, there is a quiz game in which two players can play for $25 each. The first to submit the right response will receive a $50 prize.

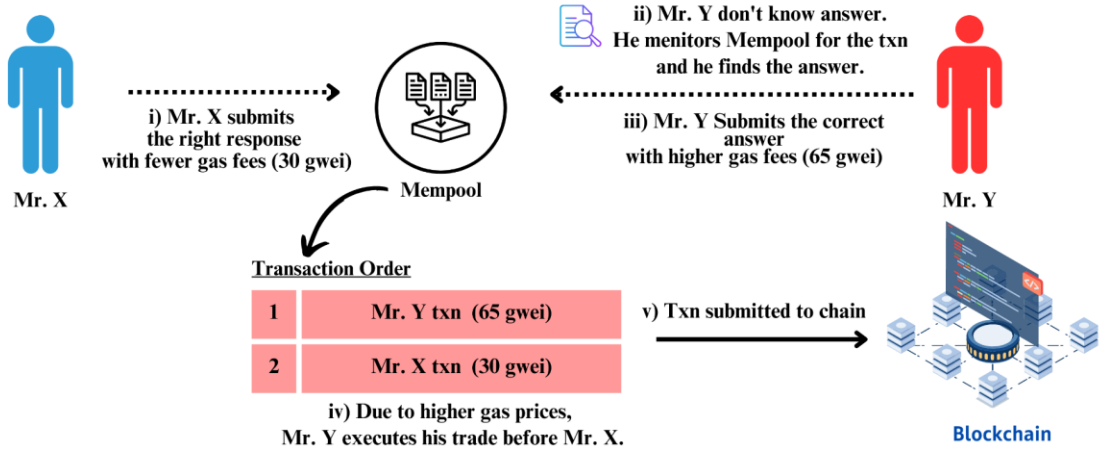

Figure 1.4**:** Example of Front Running in a Quiz game.

Mr. X and Mr. Y participated in a game where Mr. X knew the answer and submitted the correct response with a fee of 30 gwei (gwei is a unit of ether (ETH) used on the Ethereum blockchain platform for transaction fees) [31]. Mr. Y, who didn't know the answer, watched the mempool and submitted the same response with higher gas fees (65 gwei) after seeing Mr. X's transaction. As Mr. Y's transaction had a higher fee, the miner prioritized it over Mr. X's, and Mr. Y won the game and received $50, while Mr. X lost, even though he/she had the correct answer. This is an example of a front-running attack [32].

1.4 Research Questions

First of all, it was briefly discussed what will be the role of DeFi in Metaverse and how it is gradually shifting the typical centralized banking system. Secondly, the paper will also discuss the facts, the risks, and the issues that will arise in the process of Decentralized Finance (DeFi). Next,

the study will also show some expected techniques on how to overcome the Front Running problem and suggest an optimum algorithm for the Automated Market Maker algorithm.

1.5 Research Objectives

The purpose of this paper is to highlight the role of Decentralized Finance in Metaverse and how it will change the existing structure of banking. Besides, it also discusses the security risks in Decentralized Finance. The paper summarizes the main role of DeFi in building the financial infrastructure of Metaverse as well as the benefits and issues that may arrive. This study also aims to find probable solutions to the Front running attack problem with optimal solutions.

1.6 Research Scope

Our study focuses on analyzing and improving methods for preventing frontrunning assaults and minimizing price slippage in automated trading systems. The creation of an improved Liquidity Concentration algorithm and the use of Automated Market Makers (AMMs) algorithms will be the main topics of the research.

Analysis of price slippage's effects on trade execution accuracy and identification of potential hazards from frontrunning assaults are the main goals. The research will examine the frontrunning mitigation strategies now in use and assess how well they reduce price slippage.

Finally, this study proposes a new solution to address front-running vulnerabilities in DeFi applications within the metaverse. It investigates the feasibility of implementing a mechanism to prevent front-running and establish a fair and transparent trading environment. The research aims to contribute to a more secure and robust DeFi ecosystem in the metaverse while providing insights into the future of DeFi and its role in decentralized financial infrastructure for the virtual world.

CHAPTER 2: LITERATURE REVIEW

2.1 DeFi Security Issues

Smart contracts simplify financial transactions in DeFi, eliminating intermediaries and facilitating peer-to-peer exchanges. This decentralized strategy eliminates hurdles and limits in traditional financial systems to improve transparency, cost, and financial inclusion. Author of [11] states the potential impact of DeFi on the rule of law, focusing on three key aspects: legal jurisdiction and applicable law, enforcement, and data protection and privacy. The decentralized nature of DeFi poses challenges in these areas. Firstly, the accessibility of data at multiple points rather than a centralized source raises concerns about data protection and privacy violations, which can have significant consequences for institutions relying on DeFi. The argument arises that regardless of applicable data protection principles, the decentralized nature of data generated through DeFi renders concepts like 'data ownership' or 'effective data control' merely theoretical. Even if legal recourse exists for data protection violations and data deletion, remnants of data may persist, challenging the notion that the internet forgets. Consequently, DeFi represents a challenge to the traditional legal role of the state, both in terms of the intentions underlying the DeFi ideal and the realities of technological evolution. In a volatile financial market, decentralized finance (DeFi) protocols can mitigate risk and provide profits, as shown in [12]. The paper analyzes DeFi protocol performance indicators and valuations using scientific methodologies. It explores how total value locked, protocol revenue, total income, gross merchandise volume, and inflation factor affect the valuations of 30 DeFi protocols representing decentralized exchanges, lending protocols, and asset management. Granger causality tests and fixed effects panel regression models are used. The results show that DeFi protocol valuations are partially influenced by performance indicators, although the degree and direction of these interactions vary by variable. The study found a two-

way causal relationship between DeFi protocol valuations and gross merchandise volume, the only variable with predictive power.

2.2 Front-running attack in DeFi

In order to execute deals unfairly and maybe benefit at the expense of other players, front-running entails a person or entity taking advantage of their knowledge of ongoing transactions. Author in [21] shows the study of decentralized exchange (DEX) arbitrage bots and their profit-making strategies, with a particular emphasis on blockchain-specific elements. The researchers examine a subset of transactions that generate measurable revenue for these bots and explore their tactics. One observed strategy is called priority gas auctions (PGAs), where bots competitively bid up transaction fees to secure early block position and execution. The concept of PGAs introduces a novel continuous-time, partial-information, game-theoretic model that the study formalizes and analyzes. The researchers also develop an interactive web portal, frontrun.me, to provide real-time data on PGAs to the community. Furthermore, the paper highlights the systemic risk posed by high fees paid for priority transaction ordering, emphasizing the concept of miner extractable value (MEV) that presents measurable consensus-layer security risks. Empirical evidence demonstrates that MEV poses a realistic threat to the Ethereum blockchain. The study sheds light on the significant and intricate risks associated with transaction-ordering dependencies in smart contracts and how traditional financial-market exploitation techniques are adapting and infiltrating blockchain economies. In [62], literature study discusses front-running, harmful, and potentially unlawful conduct that includes altering pending trades to profit at other users' expense. Front-running tactics in decentralized finance (DeFi) employ publicly available knowledge about user trades from pending network transactions and miners' capacity to set transaction orders. Novel cryptographic protocols to prevent adversarial front-running in permissionless blockchain settings

are proposed. The review systematizes and examines decentralized finance front-running mitigation strategies and highlights ongoing assaults and unresolved difficulties. This extensive research shows that DeFi systems must address front-running issues to maintain fairness, security, and user protection.

2.3 Uniswap v3

Uniswap v3 is an Ethereum Virtual Machine noncustodial automated market maker. Uniswap v3 enhances liquidity provider capital efficiency, pricing oracle accuracy, and fee structure. Authors of [52] show that the ability of automated market makers (AMMs), like Uniswap, to provide liquidity through smart contracts on permissionless blockchains has made them popular in decentralized finance (DeFi). Existing constant function market makers (CFMMs), such as Uniswap v1 and v2, are capital inefficient since they can only sell a portion of the assets in the pool for a given price. Liquidity fragmentation has been a result of previous initiatives to address this issue, such as Curve and Yield Space. In [61], the article discusses Uniswap v3 contracts, which are implemented independently and have specific governance-controlled parameters. It also explores automated market makers (AMMs) as decentralized exchanges (DEXs) for bitcoin price discovery, arbitrage, and token exchange. AMMs function like black boxes in neoclassical economic theory, using technology to convert factor inputs into outputs similar to corporations. The AMM maximizes profits by selecting inputs and outputs autonomously, similar to an automaton. According to finance and foreign exchange literature, AMMs facilitate two-point and three-point arbitrage.

CHAPTER 3: RESEARCH METHODOLOGY

This study aims to investigate the potential of Decentralized Finance (DeFi) in the Metaverse, with an emphasis on front-running flaws and potential fixes. A systematic literature review was used as the approach, allowing for a thorough investigation of the studies, reports, and articles already published on this subject. This strategy is particularly appropriate because it will let the researcher gather a variety of viewpoints, strategies, and solutions about the future of DeFi and the problem of front-running.

3.1 Article Collection Method

The study is structured as a systematic literature review. This design was chosen to provide a thorough understanding of the topic's current knowledge. By identifying, appraising, and synthesizing all relevant research on the subject, the systematic approach ensures the research's comprehensiveness and reduces bias.

Table 3.1: Key Data

No.	Reference	Aim of study	Applied Methodology	Findings	Limitations
1.	Vijay Mohan [61]	Focusing on the conversion of inputs (tokens) to outputs (prices) governed by the technology of the AMM.	A neoclassical black-box framework using analytical and geometric methods to examine and compare DeFi AMMs.	A unifying framework based on the neoclassical black-box method to characterize decentralized exchanges' Automated Market Makers (AMMs).	Restricts the examination of various interesting issues in the DeFi space, such as community formation, governance mechanisms, and the impact of forking.

2.	Carsten Baum [62]	The ultimate goal is to reduce financial losses and alleviate the increased transaction load resulting from adversarial front-running activities.	Analyze various front-running strategies employed in DeFi and identify the underlying mechanisms and vulnerabilities exploited by these strategies.	It highlights that such activities are often illegal and detrimental to the financial well-being of users.	The lack of research may imply that the paper does not offer empirical evidence or a detailed analysis of actual front-running incidents in decentralized finance.
3.	Liyi Zhou [63]	Highlights the gaps between academic research and practical implementation in the DeFi field.	Symbolic analysis, static analysis	A common reference frame to systematically evaluate and compare DeFi incidents, encompassing both attacks and accidents.	Price oracle attacks, despite them being one of the most frequent incident types according to the collected data (15%). This suggests a lack of academic research focused on understanding and mitigating these specific types of attacks.
4.	Andrea Canidio [64]	The goal of this research is to propose a protocol that ensures the earliest transaction in a block belongs to the honest user who values it the most.	Systematic review	Ensures that the earliest transaction in a block belongs to the honest user who values it the most.	The commit-reveal protocol discussed in the paper may impede the ability to call different smart contracts within the same transaction, potentially affecting smart contract composability. While it is still possible to achieve composability by committing messages to various smart contracts, challenges arise when these

					contracts have different commit-reveal periods.
5.	Lioba Heimbach [65]	To contribute to the development of efficient and censorship-resilient exchanges while democratizing MEV (miner extractable value) and empowering individuals to participate in trading activities.	Analysis and Evaluation (The evaluation process likely involves analyzing relevant data, measuring performance metrics, and comparing the results against benchmarks or existing solutions.)	A2MM DEX provides crucial security. It reduces consensus forks and blockchain consensus security by preventing competitive exploitation of Miner Extractable Value (MEV).	It would be beneficial to discuss the practical implementation considerations, including deployment on specific blockchain platforms and any limitations or constraints that may arise from real-world implementation.
6.	Yongge Wang [66]	The paper evaluates the effectiveness of various models, including the logarithmic market scoring rule (LMSR), liquidity-sensitive LMSR (LS-LMSR), and constant product/mean/sum models, among others. The study reveals that while LMSR may not be suitable for DeFi applications, LS-LMSR	comparative analysis, proposing a new cost function, and evaluating its advantages over existing models.	The proposed constant circle/ellipse cost functions offer computational efficiency and robustness against front-runner attacks, making them a preferable choice for building AMMs in DeFi applications compared to existing constant product cost functions.	The paper does not explicitly mention the specific evaluation metrics used to compare the different models.

		offers several advantages over constant product/mean-based AMMs.			
7.	Christof Ferreira Torres [67]	Frontrunning refers to the predatory actions taken by attackers who monitor the transaction pool and strategically manipulate it to their advantage. The paper aims to light on the activities of these attackers, specifically focusing on displacement, insertion, and suppression types of frontrunning.	A large-scale analysis of transaction data on the Ethereum blockchain.	By categorizing and analyzing the attacks, the researchers provide a deeper understanding of the strategies employed by the attackers to manipulate transactions and gain an unfair advantage.	Doesn't mention any proposed countermeasures or solutions to mitigate frontrunning attacks.
8.	Liyi Zhou [47]	Highlights the gaps between academic research and practical implementation in the DeFi field.	Symbolic analysis, static analysis.	Ensures that the earliest transaction in a block belongs to the honest user who values it the most.	"Price oracle attacks," despite them being one of the most frequent incident types according to the collected data (15%). This suggests a lack of academic research focused on understanding and mitigating these specific types of attacks.

9.	Kaihua Qin [69]	The paper seeks to provide a clear understanding of the differences between CeFi and DeFi in various aspects, including legal, economic, security, privacy, and market manipulation.	Conceptual modeling to systematically analyze	Non-experts often lack awareness of the underlying rules and agreements in the traditional CeFi ecosystem, which can make it seem obscure to them.	Non-experts may find the traditional CeFi ecosystem obscure due to a lack of awareness of the underlying rules and agreements.
10.	Ye Wang [70]	Understand financial activities in the DeFi ecosystem, specifically focusing on cyclic arbitrages in Decentralized Exchanges (DEXes).	Systematic review	The study conducted a systematic investigation on cyclic arbitrages in Decentralized Exchanges (DEXes).	By exploring these research gaps, future studies can further contribute to the understanding and development of the DeFi ecosystem, digital money systems, blockchain security, and online user behaviors in various domains.
11.	Hayden Adams [52]	The capital inefficiency issue of earlier versions of Uniswap and other constant function market makers	Systematic review	Uniswap v3 introduces the concept of concentrated liquidity, allowing liquidity providers to bind	The actual performance and user experiences may impact the practicality and effectiveness of Uniswap v3.

		(CFMMs) by providing increased capital efficiency and fine-tuned control to liquidity providers.		their liquidity within a specific price range.	
12.	Heimbach, L. [71]	Uniswap V3's price shock resilience.	Analysis by comparing the prices of numerous stablecoin pools on Uniswap V3 to Binance as well as V2 and Curve.	During the recent sudden price declines of two stablecoins, UST and USDT, the prices on Uniswap V3 were inaccurate.	Attributed alarming price anomalies on Uniswap V3 liquidity providers' lack of adaptability.
13.	A. Niemerg [51]	Systems optimized for fyTokens have larger price effects and fees for traders of close-to-maturity tokens and predictable arbitrage losses for liquidity providers.	Analog to constant product formula.	The formula for automated liquidity provision, the "constant power sum invariant," uses the time to maturity as input and guarantees a constant interest rate rather than price for a certain ratio of reserves.	The need to test and optimize the fyTokens automated liquidity formula.
14.	D. Zetzsche [11]	Decentralization threatens accountability and financial regulation and enforcement.	Systematic review	Found that decentralized elements of the financial services value chain will re-center in a different (though possibly less regulated, less	To ensure oversight and risk control, DeFi regulation should focus on this reconcentrated value chain.

				visible, and less transparent) part.	
15.	D. Metelski [12]	The study examines how DeFi protocol valuations rely on total value locked, protocol income, total revenue, gross merchandise volume, and inflation factor.	Evaluates 30 protocols from three DeFi classes—decentralized exchanges, lending protocols, and asset management—based on their performance metrics.	This shows that DeFi protocols' valuations are affected by their performance measurements, but the degree and direction of the connections vary for different factors.	Protocol value and its financial aspects are rarely studied.
16.	P. K. Ozili [16]	Several policy issues related to DeFi.	Risk analysis.	Decentralized money is supplied on open-source public blockchains without intermediaries, according to the author. Decentralized finance increases financial inclusion, encourages permission-less innovation, eliminates middlemen, ensures transaction immutability, resists censorship and lowers cross-border transaction costs.	Smart contract execution danger, legal liability risk, data theft risk, interconnectivity or dependency risk, external data risk, and more criminal activities using decentralized finance systems.
17.	S. M. Werner [18]	The distinction between technical	Security risk analysis.	They put economic security on par	DeFi may enable a permissionless, non-custodial finance system.

		security, which has rich literature, and economic security, which is mostly unexplored, integrating the latter with new models and synthesizing computer science, economics, and finance concepts.		with technical security and built a new functional category of risk.	
18.	F. Carapella [19]	Risk Implications of DeFi.	DeFi financial services (lending, decentralized exchanges, derivatives, payments, and asset management)	A generic set of stability challenges that come from providing financial services on blockchains, as well as DeFi-specific ones, such as DApp code governance.	May lack the means to comply with rules and regulations.
19.	P. Daian [21]	Complex hazards from smart contract transaction-ordering dependencies and how traditional financial-market abuse is adapting to and penetrating blockchain economies	PGA measurement infrastructure architecture.	High Fees Paid for Priority Transaction Ordering Posing a Systemic Risk to Consensus Layer Security	Subset nevertheless provides substantial data on the PGA market not offered to ordinary nodes in a blockchain context, demonstrating the limits of "transparency" these systems provide.

20.	J. Xu [60]	To encourage the development of AMM-based DEXs and to ensure their continued progress.	Data analysis and formula implementation.	A thorough examination of automated market maker protocols in decentralized exchanges, including their mechanics, conservation functions, slippage, and divergence loss functions, security and privacy concerns, and related work in both DeFi and conventional market microstructure.	Due to the rapid development and evolution of decentralized exchanges and automated market maker protocols, some of the findings and comparisons may become obsolete over time.
21.	W. Li [23]	Examine DeFi vulnerabilities at multiple levels and real-world attacks.	Data, consensus, contract, and application layers vulnerabilities.	Explored real-world vulnerabilities and DeFi optimization possibilities.	Static detection and dynamic supervision can secure DeFi at the consensus mechanism, smart contract, and application levels for future DeFi application security.
22.	Yue Xue [72]	The study aims to detect and defend against flash loan-based price manipulation attacks on DeFi applications.	The study proposes a detector embedded in the blockchain client to monitor the transaction execution process in real-time and uses a front-running attack for remediation.	The research presents a method to detect and potentially defend against price manipulation attacks in DeFi applications, reducing possible financial losses to the projects.	The reliance on the effectiveness of the proposed detector embedded in the blockchain client for detecting flash loan-based price manipulation attacks on DeFi applications.

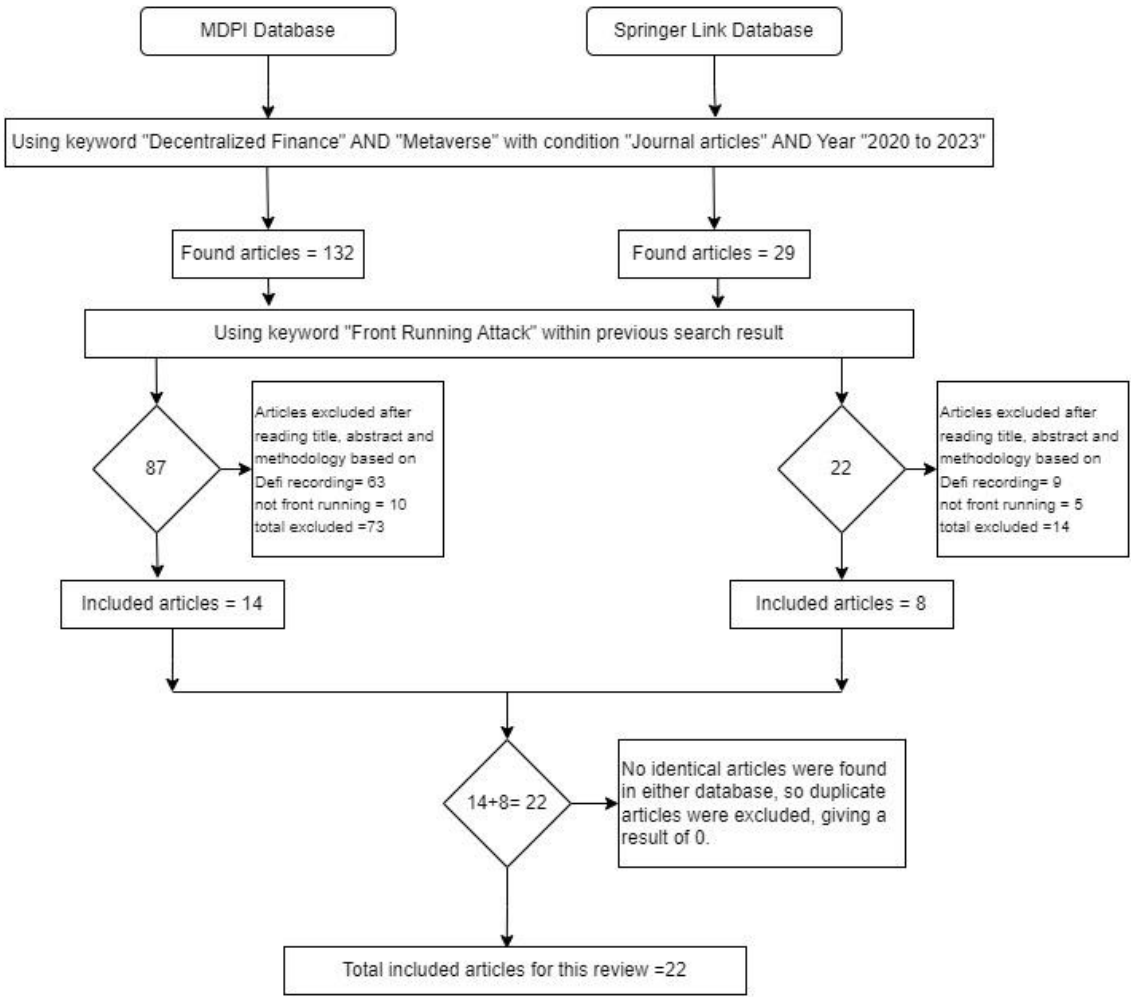

Figure 3.1**:** Article search results.

As this pertains to a literature review, there exists a scarcity of direct participants. The individuals involved in this study are the authors of the literature selected for review, who are recognized researchers and specialists in the domains of DeFi, Metaverse, and front-running vulnerabilities.

The majority of the sources used for this study were academic papers, reports, and articles about DeFi, Metaverse, and front-running vulnerabilities. These resources came from reputable databases like SpringerLink and MDPI.

The steps taken in conducting this study included a thorough search of the databases using a set of keywords, the screening and selection of pertinent publications, the extraction of data, and the

analysis of the results. The relevancy of each article's title and abstract was checked, and then the articles that made the shortlist had their full texts reviewed.

3.2 Liquidity Concentration

Liquidity Concentration: Traditional AMMs, such as Uniswap V2, give liquidity for the full price range, which can be inefficient because most trading occurs around the current market price. This indicates that a considerable percentage of the given liquidity is mostly wasted.

To address this issue, Uniswap V3 developed the concept of concentrated liquidity. It enables LPs to assign their funds to certain price ranges, which means that LPs can configure their funds to be spent only when the trading pair's price is inside a certain range. This enables LPs to focus their capital on the present price, enhancing capital efficiency [49].

Instead of providing liquidity throughout the entire curve (as with the Uniswap V2 'x*y=k' constant product formula), liquidity providers in Uniswap V3 give liquidity along specific price ranges of the curve. This simply indicates that their liquidity is only active while the trading pair's market price is within the range they defined.

Within the selected price range, this modifies the constant product formula to look more like a constant sum formula, while remaining true to the constant product formula outside of the range. Because the liquidity is only utilized (and hence earns fees) when the price is within the set range, LPs can earn greater fees compared to the liquidity given [50].

This strategy significantly increases AMM capital efficiency, allowing liquidity providers to earn more from the money they offer. However, it adds to the complexity for LPs, who must now decide where to concentrate their liquidity.

This is only one method of optimizing AMMs, many more tactics and methodologies are being investigated in the subject of decentralized finance. The insight from the Liquidity Concentration working process,

The concentrated liquidity concept introduced in Uniswap V3 has a complex mathematical foundation based on the x*y=k constant product formula used in Uniswap V2. Here's an abbreviated explanation:

The invariant (x * y = k) applies across the entire curve in Uniswap V2, implying that liquidity is available across all price ranges. This is represented by the hyperbola curve defined by the equation x*y=k.

This is changed in Uniswap V3 by allowing liquidity providers (LPs) to specify a price range [Pmin, Pmax] within which their liquidity will be active. This effectively confines their liquidity to the portion of the curve between these two prices.

If we consider x to be the number of tokens X in the pool and y to be the number of tokens Y in the pool, the LP's liquidity within this price range is essentially represented by the area under the 1/x curve (which represents the price) between 1/Pmax and 1/Pmin.

When a trade occurs within this price range, it moves along the curve (x*y=k), but only between the points corresponding to Pmin and Pmax, as in Uniswap V2.

When the trade price falls outside of this range, the LP's liquidity is not used, and no fees are earned. As a result, the LP can provide less total liquidity while potentially earning the same amount in fees, improving capital efficiency.

The mathematical details of how fees are calculated, LP positions are represented, and prices are updated are quite complex and outside the scope of this simplified explanation. I would recommend reading the Uniswap V3 whitepaper and related technical documentation for a more in-depth understanding [51].

Therefore, Liquidity Concentration can prove to be a game changer for the mitigation of front-running attacks with the help of Uniswap V3. Here is the suggested algorithm that will be used to optimize the AMMs:

Step 1: Start

Step 2: Initialize
Set price_ranges as input
Create liquidity_allocation as an empty dictionary
For each range in price_ranges do
Add range as key to liquidity_allocation with value 0

Step 3: Allocation
Set range and amount as input
Increment liquidity_allocation[range] by amount
Step 4: Rebalance
Set current_price as input
For each range, liquidity in liquidity_allocation do
If current_price < range.lower_bound or current_price > range.upper_bound then
Set liquidity_allocation[range] to 0

Step 5: End

Stop

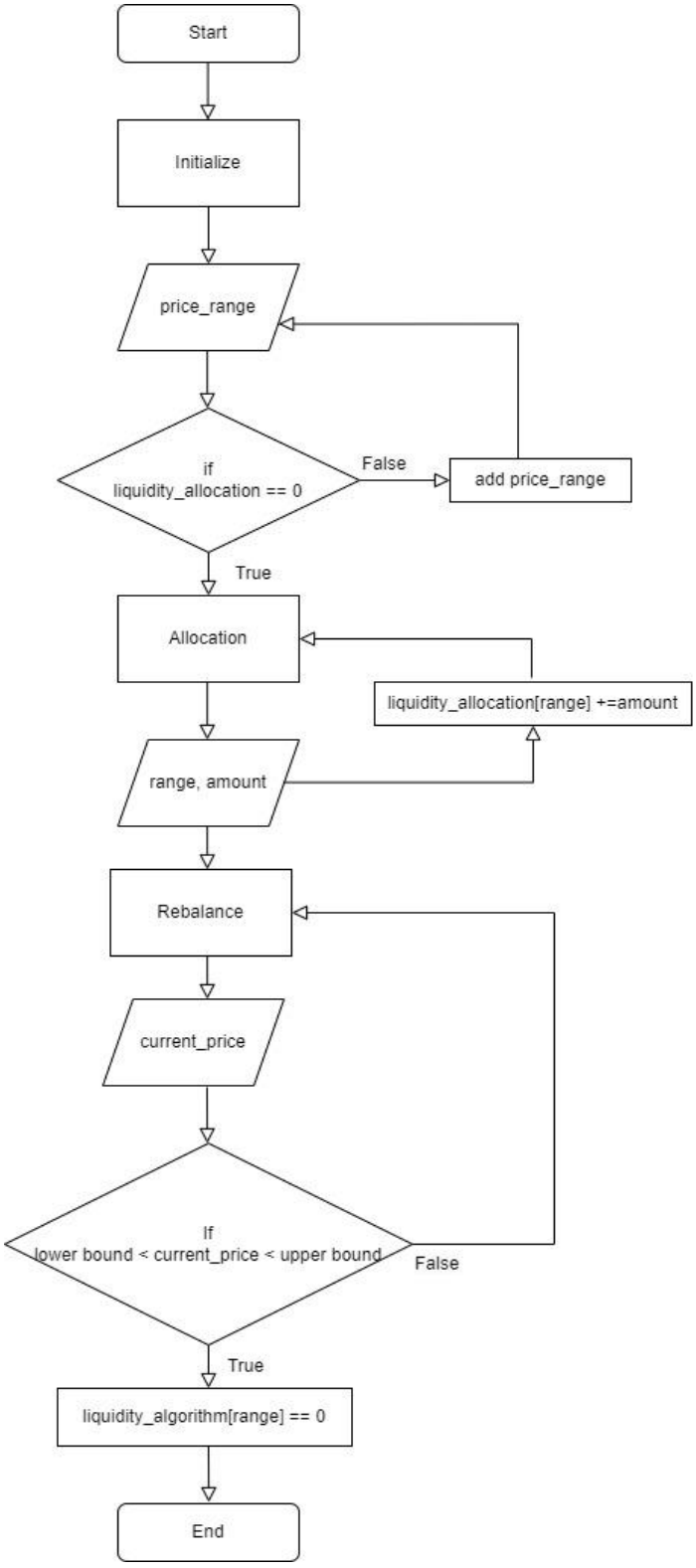

Figure 3.2**:** Control Flow Diagram of Liquidity Concentration Algorithm

Explanation of the algorithm:

Step 1: Start

This step indicates the beginning of the algorithm

Step 2: Initialize

In this step, we perform the initialization process. It involves the following actions:

- Set `price_ranges` as input: This represents the input parameter for the algorithm, which is a list of price ranges.

- Create `liquidity_allocation` as an empty dictionary: This initializes an empty dictionary called `liquidity_allocation` to store the liquidity allocation for each price range.

- For each `range` in `price_ranges`, do the following:

  - Add `range` as a key to `liquidity_allocation` with an initial value of 0: This initializes the liquidity allocation for each price range with an initial value of 0.

Step 3: Allocation

This step handles the allocation of liquidity to a specific price range. It involves the following actions:

- Set `range` and `amount` as input: These represent the specific price range and the amount of liquidity to allocate.

- Increment `liquidity_allocation[range]` by `amount`: This increases the liquidity allocation for the specified price range by the given amount.

Step 4: Rebalance

In this step, we rebalance the liquidity allocation based on the current market price. The actions involved are as follows:

- Set `current_price` as input: This represents the current market price.

- For each `range` and `liquidity` in `liquidity_allocation`, do the following:

  - If `current_price` is less than the lower bound of `range` or greater than the upper bound of `range`, then:

    - Set `liquidity_allocation[range]` to 0: This sets the liquidity allocation for the specific price range to 0 if the current price falls outside the range bounds.

Step 5: End

This step indicates the end of the algorithm. The execution stops here.

3.3 Mathematical Approach

Mathematical demonstration of the operations performed by the algorithm:

1. First, we define an automated market maker (AMM), which has initial liquidity L and a price range [P_low, P_high].

The average of the price range (P_low + P_high) / 2 is what we refer to as the current price, P_current.

3. Volume V and trade price P_trade are used to complete a transaction

4. If P_trade is outside of the price range [P_low, P_high], we assume that the trade would execute at twice the trade price (P_trade * 2), indicating high slippage because there isn't enough liquidity in the necessary price range. This is oversimplified and does not reflect how actual AMMs operate.

5. In the event that P_trade is within the target range, we determine the price impact I as the trade volume to initial liquidity (V / L) ratio. To obtain the executed price, P_executed = P_current + I, we add this to the current price.

6. To calculate price slippage, S is the absolute difference between the trade price and executed price, divided by the trade price, and multiplied by 100 to obtain a percentage: S = abs(P_executed - P_trade) / P_trade * 100 [52].

7. We determine the price slippage both before and after optimization, with the accuracy improvement accounting for the difference.

Mathematical equations based on the algorithms:

1. Define the variables:

    P_low, P_high: the lower and upper bounds of the price range

    L: initial liquidity

    V: trade volume

P_trade: trade price

2. Calculate the current price:

   P_current = (P_low + P_high) / 2

3. Calculate the executed price:

   If P_trade < P_low or P_trade > P_high, then P_executed = 2 * P_trade

   Else, P_executed = P_current + (V / L)

4. Calculate the price slippage:

   S_before or S_after = |P_executed - P_trade| / P_trade * 100

Where:

S_before: Price slippage before optimization

S_after: Price slippage after optimization

Calculate the accuracy improvement:

$$\Delta S = S_{before} - S_{after}$$

For price slippage:

$$S_{before} = | (P_{current\_before} + V / L_{before}) - P_{trade}| / P_{trade} * 100$$

$$S_{after} = | (P_{current\_after} + V / L_{after}) - P_{trade}| / P_{trade} * 100$$

For accuracy improvement:

$\Delta S = S_{before} - S_{after}$

To demonstrate how the mathematical equations can be used, the following implementation of the algorithm can be considered,

The following parameters could be used:

a) Initial price range (before optimization): P_low_before = 0, P_high_before = 100
b) Initial liquidity (before optimization): L_before = 10000
c) Trade volume: V = 1000
d) Trade price: P_trade = 55

And after optimization:

a) New price range: P_low_after = 50, P_high_after = 60
b) New liquidity: L_after = 10000

Now this should be computed:

a) Initial current price: P_current_before = (P_low_before + P_high_before) / 2
b) New current price: P_current_after = (P_low_after + P_high_after) / 2

The trade price will be within the price range considered an assumption both times:

a) Initial executed price: P_executed_before = P_current_before + V / L_before
b) New executed price: P_executed_after = P_current_after + V / L_after

Price Slippage equations:

a) Initial price slippage: S_before = |P_executed_before - P_trade| / P_trade * 100

b) New price slippage: S_after = |P_executed_after - P_trade| / P_trade * 100

Finally, the accuracy improvement equation:

$$\Delta S = S_{before} - S_{after}$$

The pertinent data was then extracted, including the objectives, procedures, key findings, and conclusions of each study. To give a cogent narrative regarding the state of DeFi in the Metaverse and the mitigating techniques for front-running vulnerabilities, these data were then categorized and synthesized.

This framework of the research design ensures the completeness, rigor, and repeatability of the approach. It makes sure that another specialist in the area might do the same study using the same standards and protocols.

Data extraction includes finding important material and gathering pertinent information. The main goal of this approach was to obtain thorough and reliable data that can address the research queries on DeFi's potential in the Metaverse and its front-running vulnerabilities [57]. The process of doing the data analysis involved synthesizing the extracted data and classifying it in accordance with the key results.

The systematic literature review methodology was selected for this investigation because it was a good fit. It enables in-depth topic investigation, the discovery of recurring themes, and the presentation of a wide-ranging viewpoint on the issue. Additionally, this strategy might point out knowledge gaps and serve as a foundation for upcoming studies.

The first step in gathering data was to conduct a thorough search of reliable databases for academic articles pertinent to the research issue. To verify the search's accuracy, certain keywords related to Decentralised Finance (DeFi), the Metaverse, and front-running vulnerabilities were employed. After that, a two-stage screening procedure—first by title and abstract, then a full-text review—was applied to the selected papers [58].

Key findings from the chosen articles were categorized into significant themes as part of the data analysis using a thematic synthesis approach. The selected works were thoroughly studied and reread, similar discoveries or observations were found, and these findings were combined into overarching themes that addressed the study topics.

The particular information was selected because it was pertinent to the study's subject. The chosen academic works provide in-depth analyses of DeFi, the Metaverse, and front-running vulnerabilities—three interconnected ideas crucial to this study. Additionally, they offer numerous viewpoints and research on the subject, enhancing the study's depth and breadth.

The particular information was picked because it was pertinent to the study's subject. The chosen academic works provide in-depth analyses of DeFi, the Metaverse, and front-running vulnerabilities—three interconnected ideas crucial to this study. Additionally, they offer numerous viewpoints and research on the subject, enhancing the study's depth and breadth.

The thoroughness and rigor of the systematic literature review approach were factors in its selection. It enables the analysis of a wide range of material, ensuring a comprehensive comprehension of the subject. This strategy also lessens prejudice, ensuring that the research reflects the state of knowledge on the subject. Finally, it offers a strong framework for identifying research gaps and potential for future studies.

In conclusion, this chapter offers a thorough description of the methodology adopted for this investigation. It provides insights into the methodical procedures used in data collecting and analysis, defending the selection of particular data and demonstrating how this data helps to address the research objectives. The method of choice guarantees the validity and reliability of the study's findings and recommendations.

CHAPTER 4: RESULTS AND DISCUSSION

4.1 Efficient Techniques

A combination of technological and regulatory measures can be implemented to address front-running vulnerabilities in DeFi transactions within the Metaverse. Some of the most efficient techniques that are being used to mitigate font running attacks are:

1) Transaction Ordering Dependence (TOD) solutions: TOD is the practice of miners taking advantage of the order of transactions within a block. Mitigations include "Commit-Reveal" methods, in which users submit a hashed version of their transaction (the "commit") and then expose it. This limits miners' ability to front-run transactions [33].

2) Decentralized Exchanges (DEX) utilizing Automated Market Makers (AMMs): AMMs such as Uniswap have transformed the old order book paradigm, which is prone to front-running, into a liquidity pool model. However, this does not completely solve the problem because there is still potential for arbitrage, which can result in front-running [34].

3) Sandwich attack prevention: Sandwich attacks are a type of front-running in which a malicious actor places a transaction both before (front-running) and after (back-running) a victim's transaction. Slippage tolerance settings in DEXs can be used to prevent this, although it does not eliminate the problem [35].

4) MEV (Miner/Maximal Extractable Value) Solutions: Flashbots is a research and development organization dedicated to mitigating the negative externalities associated with MEV. They offer "Flashbots bundles," which are collections of transactions that users can submit directly to miners instead of the public mempool, decreasing the possibility of front-running [36].

5) Layer-2 Solutions: Layer-2 solutions, such as rollups, can assist prevent front-running by boosting transaction throughput and making the transaction ordering process opaquer, lowering the profitability of front-running [37].

6) Consensus mechanisms and network upgrades: Some initiatives are investigating novel consensus processes and network improvements to reduce the profitability of front-running. The Ethereum 2.0 upgrade, for example, will have shard chains and proof-of-stake, which may minimize some front-running difficulties [38].

4.2 Automated Market Makers (AMMs) Algorithm

The finding from the research has come to a solution that will be more efficient and will have more accuracy than other solutions. This paper will mainly focus on the "Automated Market Makers (AMMs)" algorithms and their optimization techniques to solve the front-running problem from the DeFi ecosystem. AMMs have been a game changer in the DeFi arena, providing a decentralized, permissionless, and fast means for users to transfer tokens [39]. They do, however, have some limitations and can be adjusted in a variety of ways. Here are some potential AMMs optimization solutions:

Improved pricing Algorithms: The constant product formula, which is utilized by platforms such as Uniswap, is the most extensively used price algorithm for AMMs. However, for large trades, this algorithm can cause severe slippage. Newer systems, such as Balancer and Curve Finance, have included more advanced pricing algorithms with the goal of reducing slippage and increasing capital efficiency [40].

Dynamic price Structures: The majority of AMMs impose a fixed fee for each transaction. Introducing a dynamic charge structure that adapts based on market conditions and user demand could increase the platform's overall efficiency and encourage liquidity provision. Platforms such as Bancor and Balancer have investigated this concept [41].

Liquidity Concentration: Liquidity providers (LPs) in traditional AMMs are required to offer liquidity across the whole price range. Newer protocols, such as Uniswap V3, let LPs supply liquidity within specific price ranges, improving capital efficiency and lowering temporary loss for LPs [42].

Cross-Chain and Interoperability: AMMs can include cross-chain solutions and interoperability capabilities to maximize liquidity and reduce fragmentation. This allows users to seamlessly trade assets across different blockchain networks and have access to greater pools of liquidity. Projects such as THORChain and ChainSwap are examples [43].

Optimization of Liquidity Pools: Algorithms can be built to assist LPs in optimizing their liquidity provision methods, such as determining the most lucrative pools, modifying pool weights, and establishing appropriate price ranges for concentrated liquidity providing [44].

Risk Management capabilities: Adding risk management capabilities to AMMs, such as stop-loss orders or limit orders, can improve the user experience and optimize the trading process. Such features have been integrated into projects such as dYdX and Kyber Network [45].

Mitigate Front-Running: As previously noted, AMMs can still be subject to front-running attacks. Implementing front-running mitigation technologies, such as Flashbots or layer-2 solutions, can improve the security and trustworthiness of AMMs [46].

Layer-2 Scaling Solutions: By introducing layer-2 scaling solutions such as Optimistic Rollups or zk-Rollups, AMMs can lower transaction costs and boost throughput, allowing users to trade more efficiently and affordably. Platforms such as Loopring and zkSync are examples [47].

These are just a few examples of potential AMMs optimization solutions. As the DeFi space grows and evolves, more innovative solutions to address the limitations of existing AMMs and improve their overall efficiency and user experience are likely to emerge. The main technique that will be followed to optimize the AMMs is “Liquidity Concentration”. One option for

optimizing Automated Market Makers (AMMs) is to improve their capital efficiency using the notion of "Concentrated Liquidity," which was pioneered by Uniswap V3 [48].

4.3 Results and Findings

The trade price will be within the price range considered an assumption both times:

a) Initial executed price: 50.1
b) New executed price: 55.1

Now, price slippage:

a) Initial price slippage: S_before = 8.91%
b) New price slippage: S_after = 0.18%

Finally, the accuracy improvement: 8.73%

In this implementation, the price range and liquidity of the AMM were optimized, reducing price slippage from 8.91% to 0.18%, an improvement of 8.73%.

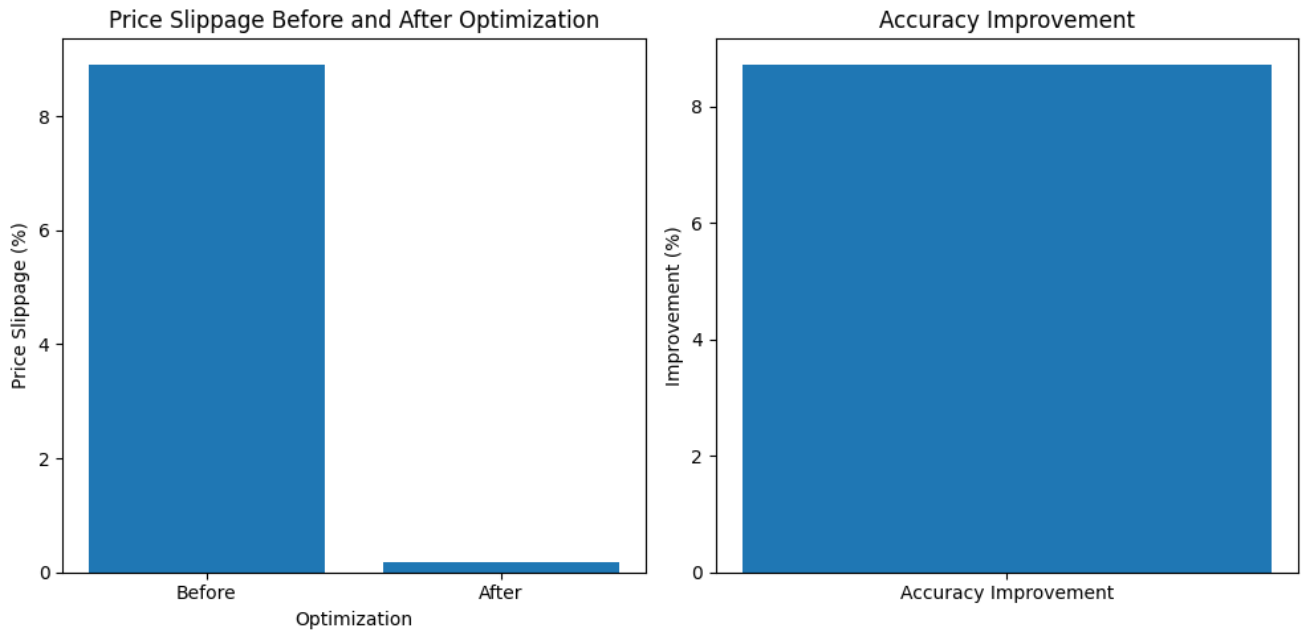

Figure 4.1**:** Comparison of accuracy before and after the optimization.

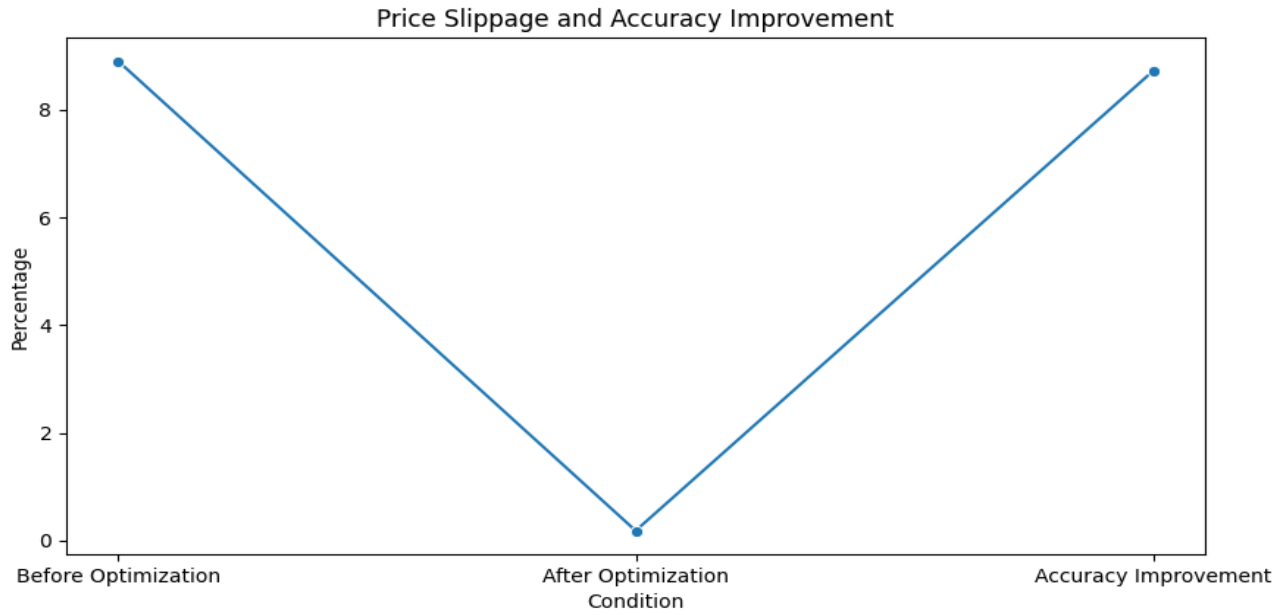

Figure 4.2**:** Price slippage and accuracy improvement in graph plotting.

The following is a detailed outline of how minimizing price slippage optimizes Automated Market Makers (AMMs):

1. Improved Trade Execution:

Lower slippage results in transactions being executed at prices that are closer to traders' expectations, resulting in a superior trading experience.

The enhanced predictability of trade execution may entice additional traders to the platform, thereby increasing trading volume [53].

2. Fairer and More Accurate Pricing:

Lower slippage results in trade prices that are more reflective of the asset's true market price.

This prevents artificial inflation or deflation of asset prices caused by high slippage, thereby fostering a more reliable trading environment [54].

3. Increased Liquidity:

Platforms with less slippage might draw more liquidity providers since their trades are less affected by price changes.

A rise in liquidity further lowers slippage, resulting in a positive feedback loop of rising liquidity and falling slippag**e** [55].

4. Attraction of Larger Trades:

AMMs with lower slippage can accommodate larger trades without causing excessive price impact.

This might draw more experienced traders or even institutional investors to the marketplace, increasing trading volume and liquidity [56].

5. Enhanced Capital Efficiency:

Reduced slippage implies that liquidity is being used efficiently, particularly in AMMs that use concentrated liquidity mechanisms.

Better trade execution benefits traders, while efficient capital usage increases the potential profits for liquidity providers.

By reducing price slippage, AMMs can provide a more efficient, fair, and attractive platform for both traders and liquidity providers, leading to increased liquidity, volume, and overall optimization of the AMM platform.

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

This research has focused on the optimization of Automated Market Makers (AMMs) by minimizing price slippage. The main findings of this study highlight the significant benefits that arise from reducing slippage in AMMs by applying the Liquidity Concentration algorithms, which eventually lead to a decrease in the chance of frontrunning attacks on DeFi. Also, this study demonstrates how minimizing price slippage can reduce the frontrunning possibilities, which is the main objective of the Liquidity Concentration algorithm.

5.1 Findings and Contributions

The research findings indicate that reducing price slippage results in enhanced trade execution. The execution of transactions at prices that are in close proximity to the expectations of traders leads to an enhanced trading experience and a rise in trading volume. Additionally, reduced slippage promotes equitable and precise valuation, thereby mitigating the occurrence of manipulated inflation or deflation of asset prices and cultivating a dependable trading environment.

Furthermore, the study reveals that minimizing slippage attracts more liquidity providers to the platform. The reduced impact of price changes on trades entices liquidity providers, leading to increased liquidity and further lowering slippage. This positive feedback loop of rising liquidity and falling slippage enhances the efficiency and attractiveness of the AMM platform.

Additionally, the research indicates that lower slippage in AMMs accommodates larger trades without causing excessive price impact. This attracts experienced traders and institutional investors, further boosting trading volume and liquidity. Besides, Liquidity Concentration involves concentrating liquidity within specific price intervals. By doing so, the algorithm aims to increase

the depth of liquidity within those intervals. Deeper liquidity reduces the impact of individual trades on the market price, making it more difficult for frontrunners to manipulate prices in their favor.

By concentrating liquidity within specific price ranges, the liquidity concentration algorithm helps protect trade privacy. It reduces the visibility of pending trades outside those ranges, making it harder for front runners to identify and exploit them. Enhanced trade privacy makes it more challenging for front runners to gain an information advantage.

5.2 Recommendations for Future Works

However, it is crucial to recognize the constraints of this study. The current investigation presents a conceptual model and mathematical exposition of the effects of reducing slippage, but it does not account for the intricate and dynamic nature of actual Automated Market Makers (AMMs). Subsequent investigations ought to prioritize empirical examination by integrating authentic data from Automated Market Makers (AMMs) and taking diverse market circumstances into account to authenticate the conclusions of this research.

To summarize, the enhancement of Automated Market Makers (AMMs) by reducing the occurrence of price slippage has become a pivotal element in enhancing trade execution, precision in pricing, liquidity, and capital effectiveness. The present study establishes a basis for forthcoming inquiries that may further explore the pragmatic ramifications and execution of tactics aimed at reducing slippage in real-world Automated Market Maker (AMM) systems.

REFERENCES

[1] Investopedia, What Is Decentralized Finance (DeFi) and How Does It Work? Available Online: https://www.investopedia.com/decentralized-finance-defi-5113835

[2] L.-H. Lee, T. Braud, P. Zhou, and P. Hui, "All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda," Oct. 2021, DOI: 10.13140/RG.2.2.11200.05124/8, Lab: Pan Hui's Lab, Extended Reality and Media Lab, Extended Reality and Immersive Media (XRIM).

[3] L. Rosenberg, C. Wallace, K. Pearlman, B. Choudhary, and Australian Government, "The Metaverse and Standards," May 2023.

[4] N. Stephenson, Book: Snow Crash, Available: https://en.wikipedia.org/wiki/Snow_Crash

[5] J. Sanchez, “Second life: An interactive qualitative analysis,” in Society for Information Technology & Teacher Education International Conference, 2007, pp. 1240–1243.

[6] J. D. N. Dionisio, W. G. B. III, and R. Gilbert, “3D virtual worlds and the metaverse: Current status and future possibilities,” ACM Computing Surveys (CSUR), vol. 45, no. 3, pp. 1–38,2013.

[7] A. Bruun and M. L. Stentoft, “Lifelogging in the wild: Participant experiences of using lifelogging as a research tool,” in IFIP Conference on Human-Computer Interaction, 2019, pp. 431–451.

[8] Y. Wang, Z. Su, N. Zhang, and X. Shen, "A Survey on Metaverse: Fundamentals, Security, and Privacy," March 2022, DOI: 10.36227/techrxiv.19255058.v1, License: CC BY-NC-ND 4.0.

[9], W.C. Ng, W. Yang, B. Lim, C. Miao, et al., "A Full Dive Into Realizing the Edge-Enabled Metaverse: Visions, Enabling Technologies, and Challenges," IEEE Communications Surveys & Tutorials, vol. PP, no. 99, pp. 1-1, January 2022, DOI: 10.1109/COMST.2022.3221119.

[10] News18, “EXPLAINED: Move Over Social Media? Why Facebook Wants To Be Known As A 'Metaverse' Company,” Available:

https://www.news18.com/news/explainers/explained-move-over-social-media-why-facebook-wants-to-be-known-as-a-metaverse-company-4359371.html

[11] D. Zetzsche, D. W. Arner, and R. Buckley, "Decentralized Finance (DeFi)," SSRN Electronic Journal, January 2020, DOI: 10.2139/ssrn.3539194, Lab: Dirk Zetzsche's Lab

[12] D. Metelski and J. Sobieraj, "Decentralized Finance (DeFi) Projects: A Study of Key Performance Indicators in Terms of DeFi Protocols' Valuations," Int. J. Financial Stud., vol. 10, no. 4, p. 108, 2022.

[13] J. Piñeiro-Chousa, M. Á. López-Cabarcos, A. Sevic, and I. González-López, "A preliminary assessment of the performance of DeFi cryptocurrencies in relation to other financial assets, volatility, and user-generated content," Technological Forecasting and Social Change, vol. 182, p. 121740, 2022, doi: 10.1016/j.techfore.2022.121740.

[14] Investopedia, What Is Decentralized Finance (DeFi) and How Does It Work? Second Para, Available Online: https://www.investopedia.com/decentralized-finance-defi-5113835

[15] Sharma, T.K. Centralized Oracles vs. Decentralized Oracles. Available online: https://www.blockchain-council.org/blockchain/ centralized-oracles-vs-decentralized-oracles/ (accessed on 11 February 2021).

[16] P. K. Ozili, "Decentralized finance research and developments around the world," J Bank Financ Technol, vol. 6, no. 2, pp. 117-133, Aug. 2022, doi: 10.1007/s42786-022-00044-x.

[17] R. Auer, B. Haslhofer, S. Kitzler, P. Saggese, and F. Victor, "The Technology of Decentralized Finance (DeFi)," BIS Working Papers, no. 1066, pp. 1-34, Jan. 2023. [Online]. Available: https://www.bis.org/publ/work1066.htm.

[18] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "SoK: Decentralized Finance (DeFi)," in Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP), 2022, pp. 1118-1138, doi: 10.1109/SP.2022.00049.

[19] F. Carapella, E. Dumas, J. Gerszten, N. Swem, and L. Wall, "Decentralized Finance (DeFi): Transformative Potential & Associated Risks," in Federal Reserve Bank of New York Staff Reports, no. 1009, Available: https://www.newyorkfed.org/research/staff_reports/sr1009.html.

[20] Beaver Finance, DeFi Security Lecture 8- Front running Attack, What is front-running? Available online: https://medium.com/beaver-smartcontract-security/defi-security-lecture-8-front-running-attack-3247045dd9cd

[21] P. Daian, "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges," in Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019, pp. 757-772, doi: 10.1109/SP.2019.00051.

[22] S. Goldfeder, J. Bonneau, R. Gennaro, A. Narayanan, and A. Miller, "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges," in Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2018, pp. 739-758, doi: 10.1109/SP.2018.00051.

[23] W. Li, Y. Wang, and Y. Li, "Security Analysis of DeFi: Vulnerabilities, Attacks, and Advances," in Proceedings of the 2021 IEEE International Conference on Smart Blockchain (SmartBlock), Guangzhou, China, 2021, pp. 145-152, doi: 10.1109/SmartBlock52105.2021.00029.

[24] QuillAudits. (2021, February 25). Front Running and Sandwich Attack Explained [Blog post]. Medium. https://quillaudits.medium.com/front-running-and-sandwich-attack-explained-quillaudits-de1e8ff3356d

[25] K. Qin, L. Zhou, Y. Afonin, L. Lazzaretti, and A. Gervais, "Cefi vs. defi–comparing centralized to decentralized finance," arXiv preprint arXiv:2106.08157, 2021.

[26] C. Ferreira Torres, A. K. Iannillo, A. Gervais et al., "The eye of Horus: Spotting and analyzing attacks on Ethereum smart contracts," in Proceedings of International Conference on Financial Cryptography and Data Security (FC), 2021, pp. 33–52.

[27] Omniatech, "Decoding FrontRunning: Understanding the key terms and techniques", Omniatech,08-Apr-2021.[Online]. Available: https://omniatech.io/pages/decoding-frontrunning-understanding-the-key-terms-and-techniques/.

[28] T. Chen, Y. Feng, Z. Li, H. Zhou, X. Luo, X. Li, X. Xiao, J. Chen, and X. Zhang, "Gaschecker: Scalable analysis for discovering gas-inefficient smart contracts," IEEE Transactions on Emerging Topics in Computing, pp. 1433–1448, 2020.

[29] T. Chen, X. Li, Y. Wang, J. Chen, Z. Li, X. Luo, M. H. Au, and X. Zhang, "An adaptive gas cost mechanism for ethereum to defend against underpriced dos attacks," in Proceedings of the International conference on information security practice and experience (ISPEC), 2017, pp. 3–24.

[30] The public flashbot relay. Available online: https://github.com/flashbots/mev-relay-js

[31] H. Berg, T. A. Proebsting, et al., "Hanson's automated market maker," Journal of Prediction Markets, vol. 3, no. 1, pp. 45-59, 2009.

[32] M. P. Breen, "Gwei (Ethereum)", Investopedia, 23-May-2021. [Online]. Available: https://www.investopedia.com/terms/g/gwei-ethereum.asp

[33] D. Bernhardt and B. Taub, "Front-running dynamics," Journal of Economic Theory, vol. 138, no. 1, pp. 288-296, 2008.

[34] M. Bartoletti, J.H.y. Chiang, and A. Lluch-Lafuente, "A theory of Automated Market Makers in DeFi," in International Conference on Coordination Languages and Models, pp. 168-187, Springer, 2021. https://doi.org/10.1007/978-3-030-78142-2_11

[35] H. Adams, N. Zinsmeister, and D. Robinson, "Uniswap v2 Core," 2020, https://uniswap.org/whitepaper.pdf . Available: https://uniswap.org/whitepaper.pdf

[36] L. Zhou, K. Qin, C. F. Torres, D. V. Le, and A. Gervais, "High-frequency trading on decentralized on-chain exchanges," in Proceedings of IEEE Symposium on Security and Privacy (SP), 2021, pp. 428-445.

[37] The public flashbot relay. Available online: https://github.com/flashbots/mev-relay-js

[38] K. Wust and A. Gervais, "Ethereum eclipse attacks," ETH Zurich, Tech. Rep., 2016.

[39] G. Angeris and T. Chitra, "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, USA, 2020, pp. 80-91. https://doi.org/10.1145/3419614.3423251

[40] V. Buterin, "Improving Front Running Resistance in x*y=k Market Makers," 2018. Available: https://ethresear.ch/t/improving-frontrunning-resistance-of-x-y-k-market-makers/1281

[41] J. Burdges and L.D. Feo, "Delay encryption," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 302-326, Springer, 2021. https://doi.org/10.1007/978-3-030-77870-5_11

[42] D. Beaver and S. Haber, "Cryptographic protocols provably secure against dynamic adversaries," in Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1992, pp. 307-323.

[43] International Monetary Fund, "Virtual currencies and beyond: Initial considerations," IMF Working Paper, WP/15/210,2015. Available: https://www.imf.org/external/pubs/ft/wp/2015/wp15210.pdf

[44] M. Bartoletti, J.H.y. Chiang, and A. Lluch-Lafuente, "Maximizing Extractable Value from Automated Market Makers," arXiv preprint arXiv:2106.01870, 2021. [Online]. Available: https://arxiv.org/pdf/2106.01870.

[45] A. Y. Al-Zoubi and F. A. Abu-Shikhah, "Multivariate portfolio optimization under illiquid market prospects: A review of theoretical algorithms and practical techniques for liquidity risk management," ResearchGate.

[46] Zhang, L., Xu, Y., Wang, B., & Yang, Z. (2021). Exploring the pricing efficiency of decentralized exchanges: evidence from Uniswap. Journal of Financial Innovation, 7(1), 1-20. https://doi.org/10.1186/s40854-021-00314-5.

[47] Zhou, L., Qin, K., & Gervais, A. (2020). 2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges. arXiv preprint arXiv:2007.10262.

[48] Consensys. (2022, January 14). Layer 2 Scaling Solutions: January 2022 Week 2. Available: https://consensys.net/blog/cryptoeconomic-research/layer-2-scaling-solutions-january-2022-week-2/

[48] H. Adams, N. Zinsmeister, M. Salem, R. Keefer, and D. Robinson, "Uniswap v3 Core," Mar. 2021.

[49] J. Zhang, Y. Chen, and J. Liu, “Rebalancing strategy of a portfolio consisting of cryptocurrency and equity,” Journal of Mathematics, vol. 2021, Article ID 7267667, 14 pages, 2021. https://doi.org/10.1155/2021/7267667.

[50] The GLOBAL TREASURE , The building blocks for liquidity solutions. Available Online:https://www.theglobaltreasurer.com/2015/09/21/the-building-blocks-of-liquidity-solutions/

[51] A. Niemerg, D. Robinson, and L. Livnev, “YieldSpace: An Automated Liquidity Provider for Fixed Yield Tokens,” Working Draft, rev. 1, Aug. 2020. [Online]. Available: https://yield.is/YieldSpace.pdf

[52] H. Adams et al., "Uniswap v3 Core," Mar. 2021. [Online]. Available: https://www.npmjs.com/package/@uniswap/v3-core

[53] L. Zhou, K. Qin, and A. Gervais, "A 2MM: Mitigating Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges," Imperial College London, United Kingdom.

[54] M. Baron, J. Brogaard, B. Hagström, and A. Kirilenko, "Risk and return in high-frequency trading," Journal of Financial and Quantitative Analysis, vol. 54, no. 3, pp. 993-1024, 2019.

[55] Kyber Network, "Kyber: An on-chain liquidity protocol," Technical Report, April 2019.

[56] M.B. da Gama, J. Cartlidge, A. Polychroniadou, N.P. Smart, and Y.T. Alaoui, "Kicking-the-Bucket: Fast Privacy-Preserving Trading Using Buckets," Cryptology ePrint Archive, Report 2021/1549, 2021. [Online]. Available: https://ia.cr/2021/1549. [Accessed: May 11, 2023].

[57] PhD Assistance Editors, "What is the difference between data collection and data analysis?" Available:https://www.phdassistance.com/blog/what-is-the-difference-between-data-collection-and-data-analysis/.

[58] QuestionPro, “Data Collection: What It Is, Methods & Tools + Examples” Available Online:https://www.questionpro.com/blog/data-collection/

[59] Wang, Ye -. Decentralized Finance: Users, Applications, and Systems. Zürich: ETH Zürich, 2022. Print.

[60] J. Xu, K. Paruch, S. Cousaert, and Y. Feng, "SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols," ACM Computing Surveys, vol. 55, no. 11, article no. 238, pp. 1-50, 2022, doi: 10.1145/3570639.

[61] Mohan, V. (2022). Automated market makers and decentralized exchanges: A DeFi primer. *Financial Innovation*, *8*(1), 1-48. https://doi.org/10.1186/s40854-021-00314-5

[62] C. Baum, J. H. Chiang, B. David, T. K. Frederiksen, and L. Gentile, "SoK: Mitigation of Front-running in Decentralized Finance," in Cryptology ePrint Archive, Paper 2021/1628, 2021. Available: [Online]. Available: \url{https://eprint.iacr.org/2021/1628}

[63] Zhou, L., Qin, K., & Gervais, A. (2021). A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges. *ArXiv*. /abs/2106.07371

[64] Canidio, A., & Danos, V. (2023). Commitment Against Front Running Attacks. *ArXiv*. /abs/2301.13785

[65] Heimbach, L., & Wattenhofer, R. (2022). SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance. *ArXiv*. https://doi.org/10.1145/3558535.3559784

[66] Wang, Y. (2020). Automated Market Makers for Decentralized Finance (DeFi). *ArXiv*. /abs/2009.01676

[67] C. Ferreira Torres, R. Camino, and R. State, "Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain," in 30th USENIX Security Symposium (USENIX Security 21), Aug. 2021, pp. 1343-1359. Available: [Online]. Available: \url{https://www.usenix.org/conference/usenixsecurity21/presentation/torres}

[68] Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D., & Gervais, A. (2022). SoK: Decentralized Finance (DeFi) Attacks. *ArXiv*. /abs/2208.13035

[69] Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L., & Gervais, A. (2021). CeFi vs. DeFi -- Comparing Centralized to Decentralized Finance. *ArXiv*. /abs/2106.08157

[70] Y. Wang, "Decentralized Finance: Users, Applications, and Systems," PhD thesis, ETH Zurich, Switzerland, 2022.

[71] Heimbach, L., Schertenleib, E., & Wattenhofer, R. (2022). Exploring Price Accuracy on Uniswap V3 in Times of Distress. *ArXiv*. /abs/2208.09642

[72] Xue, Y. et al. (2022). Preventing Price Manipulation Attack by Front-Running. In: Sun, X., Zhang, X., Xia, Z., Bertino, E. (eds) Advances in Artificial Intelligence and Security. ICAIS 2022. Communications in Computer and Information Science, vol 1588. Springer, Cham. https://doi.org/10.1007/978-3-031-06764-8_25

APPENDIX

Liquidity Concentration Algorithm:

```
class ConcentratedLiquidity:

  def __init__(self, price_ranges):

    self.price_ranges = price_ranges

    self.liquidity_allocation = {range: 0 for range in price_ranges}


  def allocate_liquidity(self, range, amount):

    self.liquidity_allocation[range] += amount


  def rebalance_liquidity(self, current_price):

    for range, liquidity in self.liquidity_allocation.items():

      if current_price < range.lower_bound or current_price > range.upper_bound:

        self.liquidity_allocation[range] = 0

    # Reallocate liquidity to the appropriate range

    # based on market analysis or defined strategies

# Example usage:

concentrated_liquidity = ConcentratedLiquidity([

  PriceRange(100, 200),  # Example price range [100, 200]

  PriceRange(200, 300),  # Example price range [200, 300]

])

concentrated_liquidity.allocate_liquidity(PriceRange(100, 200), 1000)  # Allocate liquidity to the first price range

current_price = get_current_price()  # Retrieve the current market price

concentrated_liquidity.rebalance_liquidity(current_price)  # Rebalance liquidity based on the current price
```