*electronics*

MDPI

*Article*

# Decentralized Exchange Transaction Analysis and Maximal Extractable Value Attack Identification: Focusing on Uniswap USDC3

**Nakhoon Choi [1] and Heeyoul Kim [2,*]**

[1] Department of Computer Science, Kyonggi University, Suwon 16227, Republic of Korea; nakhoon.choi@kyonggi.ac.kr
[2] Division of Computer Science and Engineering, Kyonggi University, Suwon 16227, Republic of Korea
* Correspondence: heeyoul.kim@kyonggi.ac.kr

**Abstract:** With the advancement of blockchain technology and growing concerns about the vulnerabilities and mistrust in centralized financial services, decentralized finance (DeFi) and decentralized exchanges (DEXs) have emerged as promising alternatives. This paper delves into the challenges and issues within DeFi, with a particular focus on Uniswap. We highlight the susceptibility to Maximal Extractable Value (MEV) attacks, providing a background on the current state of DeFi and DEXs. Our approach includes a detailed transaction analysis on Uniswap to identify and analyze MEV attack patterns, alongside a method for detecting bots. The results offer critical insights into the nature of various attacks in DEXs and the correlation between internal and external blockchain events and MEV attack patterns. This research provides valuable guidelines for enhancing DEX security and mitigating MEV risks, serving as an essential resource for stakeholders in the DeFi ecosystem.

**Keywords:** decentralized finance; decentralized exchange; DEX; MEV; Uniswap; USDC3



**Citation:** Choi, N.; Kim, H. Decentralized Exchange Transaction Analysis and Maximal Extractable Value Attack Identification: Focusing on Uniswap USDC3. *Electronics* **2024**, *13*, 1098. https://doi.org/10.3390/electronics13061098

Academic Editor: Paulo Ferreira

Received: 1 February 2024
Revised: 3 March 2024
Accepted: 14 March 2024
Published: 16 March 2024



## 1. Introduction

Decentralized finance (DeFi) and decentralized exchange (DEX), which are emerging with the development of blockchain technology, represent an innovative turning point in financial technology by providing a platform for trading cryptocurrency without centralized authority, servers, and administrators. As blockchain technology develops, its by-products, cryptocurrency and tokens such as ERC-20 and ERC-721, are being used. The financial market provides a centralized exchange (CEX) for cryptocurrency trading. However, various problems arose, including a series of hacking of exchanges, asset theft, and lack of reliability in the judgment of centralized exchanges. Blockchain researchers proposed DeFi and DEX, financial technologies, to address the problems arising from these centralized services and to strengthen the spirit of blockchain, which is decentralization. DeFi provides blockchain-based financial services that replace traditional centralized financial systems, and DEX provides users with the opportunity to directly exchange crypto assets in this new financial ecosystem. Decentralized finance promotes P2P transactions through blockchain smart contracts, strengthens transparency and security of transactions, and excludes risks such as malicious actions by administrators and authority theft that occur in centralized exchanges. This is dramatically improving the transparency and accessibility of financial transactions [1]. DeFi and DEX are expanding the availability of financial services globally, which is seen as a significant challenge to the traditional financial system [2].

DeFi and DEX are receiving a lot of attention amid new technological innovations in blockchain, but at the same time, they are facing various security threats. Various attack techniques such as smart contract vulnerabilities, market manipulation, and front-running are emerging as major threats in this field [3,4]. The emergence of MEV (Maximal Extractable Value) bots, one of the major threats, is gaining profits through vulnerabilities

in decentralized finance and causing losses in commissions and exchange fees for users' transaction execution. Various attempts by MEV to target the security vulnerabilities of the blockchain itself or the vulnerabilities of the DEX have been discovered, damaging transaction integrity and fairness. Security issues and attacks on decentralized financial services expose users' assets to direct risk undermine the reliability of blockchain platforms and services and affect the stability of the entire market [5]. For a fair and trustworthy financial environment, thorough analysis and understanding of the security vulnerabilities and attack methods of distributed finance are essential. This analysis will provide an important foundation for the sustainable growth and development of DeFi and DEX.

This paper provides analysis of DEX transaction data to identify various attack techniques targeting DeFi, a blockchain financial service, and DEX system. Through this, we identify market trends, user behavior, and security issues and seek ways to strengthen security and operate the market efficiently in this field. In addition, through the analysis of DEX transaction data, we identify methods of MEV attacks based on front learning techniques and confirm attack behavior and DEX arbitrage attack. Through this, we analyze DEX transaction trends and MEV-bot patterns. For this purpose, we extracted and analyzed transactions from the USCD/WETH token pair pool of Uniswap, the largest DEX, until 2023. In trading history, the attack volume of arbitrage and front-running (Sush as Sandwich) MEV-bot amounts to USD 480 million out of the total daily average trading volume of USD 1 billion, accounting for 45% of the total daily average volume. We seek to shed new light on the severity of MEV attackers on DEXs through several attack volume measurements along with methods to identify these attacker transactions. This analysis and research will not only contribute to improving the stability and transparency of DeFi and DEX but will also serve as an important reference for academic research and industrial practice in this field. The transaction data collected and analyzed in this paper can be found on our GitHub at the following URL: [https://github.com/skg4463/MDPI_DEX-MEV_transaction_analysis] (accessed on 31 January 2024).

The structure of this paper aims to explain blockchain decentralized finance and decentralized exchanges in Section 2, and to analyze vulnerabilities in blockchain and decentralized exchanges and attack techniques based on them in Section 3. Section 4 introduces the data collection and processing methods for DEX analysis and the analysis results according to the processing, and Section 5 presents the conclusion.

## 2. Related Research on Dex Attacks

This paper investigates the latest research trends on various attacks to analyze security issues and attack types in decentralized finance. The DeFi ecosystem is exposed to various security vulnerabilities and attacks, and research to respond to these is actively underway.

Alam et al. [6] analyzed the impact of front-running attacks occurring in DeFi systems within the metaverse. This study highlights the impact of front-running attacks on the reliability and fairness of DeFi markets. Xiang et al. [7] empirically analyzed cases of security attacks that occurred during the development of DeFi projects. This study details the security vulnerabilities and attack methods of DeFi systems.

Wu et al. [3] developed a system to detect price manipulation attacks in the DeFi market. This study identifies the semantics of DeFi transactions and presents a methodology to detect attacks based on this. Arora et al. [8] conducted research to develop a security protocol to respond to oracle manipulation attacks. This study proposes ways to address vulnerabilities in oracle systems and strengthen the reliability of DeFi platforms.

Huang et al. [9] analyzed the interaction between AI technology and DeFi security. This study explores how AI systems may be exposed to adversarial attacks in the DeFi environment. Parhizkari et al. [10] conducted research to develop a rapid identification and response plan for victim addresses during DeFi attacks. This study highlights the importance of real-time attack detection and prevention systems.

Chaliasos, S., et al. [11] conducted an evaluation and investigation on the effectiveness of smart contracts and DeFi security tools. The study points out the need for improvements

in security tools and training of practitioners. Finally, Kaur et al. [12] provide a comprehensive analysis of cybersecurity management strategies for DeFi infrastructure. This research focuses on identifying security vulnerabilities in DeFi systems and developing comprehensive management strategies.

Table 1 offers a concise overview of the proposed solutions for various types of attacks in DeFi, categorizing them based on whether they exploit vulnerabilities in the blockchain environment or are specific to DEX and DeFi environments. It also details the impact of these attacks, providing a clear picture of the challenges and solutions in DeFi security.

**Table 1.** Analysis of recent trends in related research on DeFi attacks.

| Type of Attack | Exploited Vulnerability | Damage Scale | Proposed Solution |
|---|---|---|---|
| Front-running Attacks [6] | DeFi Environment in Metaverse | Degrades trust in DeFi transactions within the Metaverse, increases unfair trading practices | Enhancing blockchain transparency, reducing latency |
| Various Security Attacks (hacking, phishing, etc.) [7] | General DeFi Environment | Financial losses in DeFi projects, diminishing user trust | Enhanced security protocols, user education |
| Price Manipulation Attacks [3] | DeFi Market Environment | Investor losses and reduced market integrity due to market manipulation | Advanced transaction analysis tools, strengthened regulations |
| Oracle Manipulation Attacks [8] | Specific to DeFi platforms using Oracles | Compromised data accuracy and reliability in DeFi systems, financial damages | Sophisticated oracle systems, oracle data verification |
| Adversarial AI Attacks [9] | AI Systems within DeFi | Information leaks and system errors due to AI system vulnerabilities | Strengthening AI system security, continuous updating |
| General DeFi Attacks [10] | General DeFi Environment | Inability to minimize immediate damages due to failure in real-time attack detection | Real-time detection systems, rapid response mechanisms |
| Smart Contract Vulnerabilities [11] | Blockchain and Smart Contract Environment | Financial losses and system malfunctions due to bugs and vulnerabilities in smart contracts | Security tool improvements, code auditing |
| Cybersecurity Management [12] | Overall DeFi Infrastructure | Various security threats due to overall vulnerabilities in DeFi infrastructures | Comprehensive cybersecurity strategies, risk assessment |

The purpose of this study is to analyze and investigate various security attacks occurring in decentralized finance (DeFi) and decentralized exchanges (DEX). Through this analysis, we identify security vulnerabilities in DeFi and DEX systems, identify risks that may arise through them, and propose effective security strategies to respond to them. Recent studies have extensively covered various security threats and vulnerabilities facing DeFi and DEX systems. These studies are analyzing in-depth front-running attacks, various hacking and phishing attacks, oracle manipulation attacks, and hostile AI attacks that can occur in the DeFi environment. It also includes research on smart contract vulnerabilities and cybersecurity management. Attacks against security vulnerabilities in these DeFi and DEX systems are very diverse and are changing in real time. However, because the vulnerabilities being attacked are based on the structural vulnerabilities of blockchain and DEX, it is necessary to understand these vulnerabilities in detail. Therefore, this paper investigates and analyzes these vulnerabilities and analyzes the type, form, and scale of attacks that occur according to these vulnerabilities.

## 3. Blockchain and Decentralized Finance and Decentralized Exchange

Blockchain and decentralized finance are key elements of modern financial technology, providing innovative approaches to overcome the limitations of traditional financial systems. Blockchain ensures the integrity and security of data through the separate storage of information and encrypted transaction records. Each transaction is recorded in a unit of data known as a block, and these blocks are linked in a chain, making them difficult to manipulate. Each block is linked to the hash of the previous block, ensuring that all transactions on the blockchain are linked in a chronological order. The work on the network that connects each block of the blockchain to the chain is called consensus, and various consensus algorithms such as PoW, PoS, and DpoS exist depending on the structure and characteristics of the blockchain [13]. Blocks created by block generators elected through this consensus are transmitted to all participants in the network. Network participants maintain a transparent and open network to all participants on the network by verifying and recording the validity of transactions. This process creates a trustworthy trading environment without the need for centralized institutions or intermediaries. Cryptocurrencies generated as block creation rewards and token-type cryptocurrencies such as ERC-20 and ERC-721 generated through smart contracts are traded through order book-based centralized exchange services. However, there are problems with relying on administrators, such as asset damage due to frequent hacking of the exchange itself and cryptocurrency registration based on the judgment of the central exchange. To this end, DEX emerged as an attempt to create a decentralized exchange through smart contracts.

Decentralized finance provides financial services based on blockchain in a decentralized environment without administrators. Unlike traditional financial services performed through banks or exchange companies, DeFi automates financial transactions through smart contracts and allows users to directly participate in transactions. EtherDelta, an early DEX project on Ethereum, proposed a method that connects buyers and sellers based on an order book and supports matching bid prices and minimum prices. However, order book-based DEX required too much gas fees for transaction execution, and because buy and sell transactions were registered in advance, there was a significant burden in creating or canceling transactions. Additionally, problems with usability and scalability arose due to a lack of liquidity. Order book-based exchanges were unsuitable for the blockchain environment, and to solve this problem, an Automated Market Marker (AMM)-based decentralized exchange was proposed [14]. AMM allows anyone to provide liquidity to the exchange and supports trading between users at a price determined by an algorithm based on liquidity. The total DEX trading volume in 2023 is approximately USD 889 billion, and the total number of traders is approximately 43.2 million. For DEX analysis, we perform analysis on Uniswap, which has the largest trading volume and number of users. Uniswap is an open-source DeFi project, and exchanges such as SushiSwap have a similar structure because they are based on open-source Uniswap. Uniswap is an AMM-based exchange that consists of a pricing algorithm, liquidity provider, and token pair. Uniswap uses the CPMM (Constant Product Market Maker) model among the AMM models. CPMM determines the price through Equation (1), a constant multiplication formula, where X and Y refer to the quantity of each token (x, y), and K refers to the product of the quantities.

$$X \times Y = K \tag{1}$$

CPMM is an algorithm in which the product of X and Y, which changes after performing all transactions within liquidity, is always maintained at a constant K. When exchanging X for Y in Token Fairpool, the amount of X decreases, and the amount of Y increases. Accordingly, the price of x falls, the price of y rises, and K remains constant. Figure 1 shows an example of a CPMM-based transaction. The user perceived the price of DAI compared to ETH before the transaction as 1:50, but temporary price fluctuations (slippage) [15] that caused a significant difference occurred due to CPMM. This slippage occurs as the amount of liquidity provided to the exchange increases (the larger K), and lower is the amount of

price fluctuation that occurs when executing a transaction. Therefore, exchanges provide transaction fees to liquidity providers to increase liquidity.

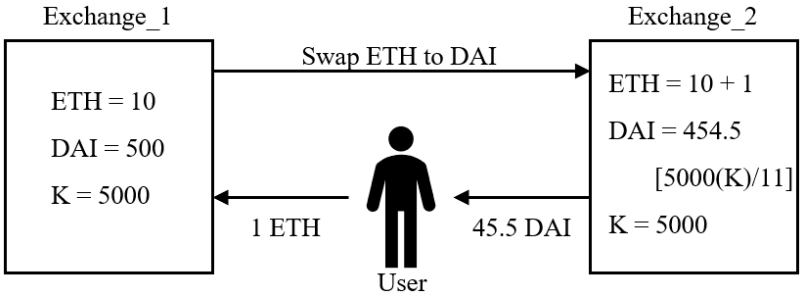



**Figure 1.** Example of token trading in CPMM.

However, Uniswap is a financial exchange serviced on blockchain, and there are various problems that arise when using blockchain and vulnerabilities depending on the exchange structure and project structure. We perform analysis on the structural vulnerabilities and various types of attacks of these blockchain platforms and DEXs.

## 4. Analysis of Decentralized Exchange Vulnerabilities and Attack Types

There are various types of attacks targeting DEX users' assets. There is a debate among the blockchain community and researchers as to whether stealing profits through methods such as arbitrage and front-running through the structural weaknesses of DEX is an attack or a legitimate profit activity [16]. However, we would like to define this as an attack and analyze it, as the benefit arising from this behavior is the process of stealing other users' assets. Such 'attacks' generate profits by intervening in the purchasing process of ordinary users and forcing them to conduct transactions at a higher price. A DEX attack is an act that creates unfair transactions by abusing the transparency of the blockchain that supports the reliability of the DEX and destroys the reliability of the blockchain platform environment beyond the DEX. MEV-bot is carrying out these attacks on all transactions above a certain size that occur on DEX and is forcing users to suffer losses [17]. In this section, we analyze various types of attacks that occur in DEX and identify their structural causes.

### *4.1. Structural Vulnerabilities in Blockchain*

DEX based on blockchain has the same structural characteristics as blockchain. A major feature of the blockchain's block generation mechanism is MEV (Miner Extractable Value). Blockchain users' transactions are not processed immediately, but are held in the mempool, which is the transaction waiting space for block generator candidates. They are selected by the elected block generator, inserted into a specific block, and then processed into blocks to join the blockchain. The block generator (Ethereum Validator) elected in the round first selects transactions that pay the highest fee (gas) among transactions pending in the mempool and attempts to process them into blocks. Miners, like MEV-bots, pursue maximum profits. However, as most of the MEV is taken by arbitrage bots or liquidation bots of lending protocols, MEV is currently called Maximal Extractable Value. Figure 2 shows transaction selection according to the miner's block creation mechanism in the blockchain.

Depending on the MEV (Miner Extractable Value) transaction selection in Figure 2, the block generator can confirm that the transaction paying the highest fee in the mempool is added to the block. The mempool, a temporary public transaction list waiting to be mined, is made public by blockchain transparency and can be accessed through the node application. Front-running attacks are based on this and can check the transaction contents of the mempool, which is a public transaction waiting list, and transmit transactions that are processed before existing transactions to the network. This attack method was first presented in Flash boys 2.0 [18] in 2019. The attacker, MEV-bot, continuously monitors transactions sent to the mempool, and when a transaction that satisfies certain conditions

is detected, it simulates the results of the transaction in advance. Once a transaction with conditions to generate profit is confirmed, the manipulated transaction is executed first to generate profit. Depending on the MEV transaction selection in the block creation mechanism, the processing order of the transaction may differ from the time the transaction was actually transmitted to the network. However, activities such as token swaps and liquidity provision in DEX cause volatility in market value depending on prior actions and time information. Users may incur losses due to actual transaction performance that differs from the intended transaction due to these factors.

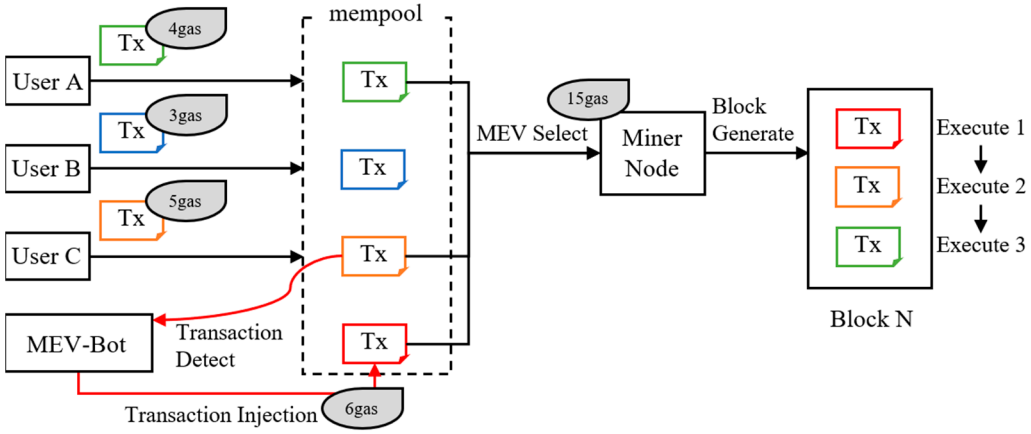



**Figure 2.** Blockchain block miner's MEV (Miner Extractable Value) transaction selection and front-running attack.

Sandwich attack is a form of front-running attack targeting the AMM model of DEX and is the most common front-running-based attack in the DEX ecosystem. To explain the sandwich attack intuitively, when a purchase transaction is scheduled to be executed under certain conditions, MEV-bot first purchases the same token and sells it immediately after the transaction is executed, generating profit equal to the difference. Figure 3 is a diagram that intuitively expresses an example of a sandwich attack.

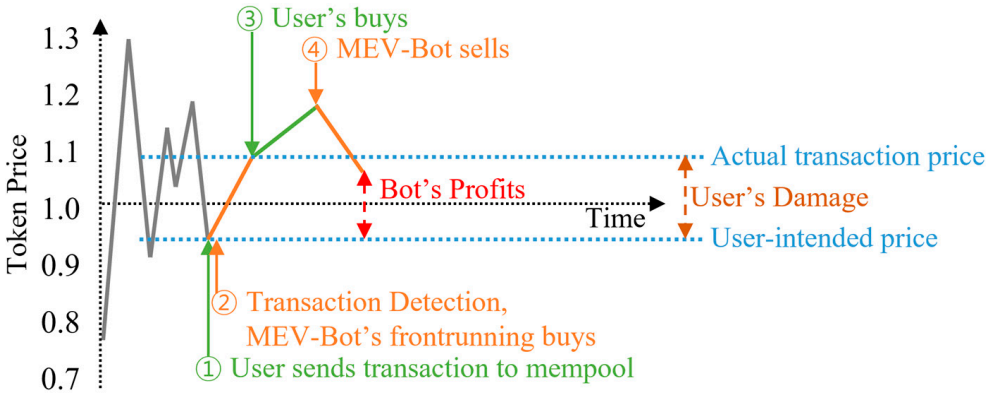



**Figure 3.** Execution process and profit generation section of sandwich attack.

The sequence and process of the front-running-based sandwich attack in Figure 3 are explained in detail as follows:

1. General users using DEX submit transactions for asset swaps, and the transactions are recorded in the blockchain mempool;
2. The attacker monitors the blockchain mempool and detects large pending transactions that are expected to significantly change the price of the liquidity pool. Additionally, upon detection, the attacker artificially increases the price of the token according to the AMM by submitting a buy order for the same token with a higher commission (gas) before the user's transaction is processed;

3. Users purchase tokens at a higher price than the intended price, and after transaction processing, the token price increases further depending on the transaction size;
4. Immediately after the victim's transaction, the attacker sells the tokens purchased in the previous step at an increased price and realizes a profit equal to the difference.

In Figure 3, MEV-bot is expressed in red letters, and for convenience, it is displayed so that it can be checked intuitively. If the bot's profit is displayed more clearly, it is expressed as the amount actually used in the bot's token purchase stage and the actual sold price in the sales stage according to the CPMM in Equation (1). The profit of MEV-bot is expressed as Equation (2). In Equation (2), $P$ is the expected profit of MEV-bot, $B_x$ is the quantity of token X purchased by the user, $B'_x$ is the quantity of token X purchased by the attacker, and $x$ is the quantity of tokens available in Token Fair's liquidity pool.

$$P = B'_x - x\frac{R}{1-R} \tag{2}$$

$$R = \frac{x}{x + B_x} - \frac{x}{x + B_x + B'_x} \tag{3}$$

According to Equations (2) and (3), the lower the quantity of tokens in the liquidity pool, $x$, the higher the profits. However, if interpreted more intuitively, the increase in profits is confirmed to be proportional to the quantity of tokens purchased by attackers and users. Unlike arbitrage bots, sandwich attacks cannot occur in a single transaction. However, through relay services such as Universal Router [19] and Flashbot [20], multiple attack transactions allow the buy-sell attack logic to be closely performed. A typical sandwich attack is performed with the logic of detecting a user's purchase and purchasing it in advance, but in extremely rare cases, an attack is discovered in which the attacker sells and then repurchases the assets he or she holds. In this case, it is recorded as a very rare case in that the attacker must have in advance held a cryptocurrency asset with price volatility. In the case of a sandwich attack, a back-running attack is performed together with a front-running attack. Contrary to front-running, back-running attacks are aimed at processing the victim's transactions immediately after or further after they are confirmed in the mempool. To achieve this, MEV-bot creates transactions with a fee that is approximately equal to or slightly lower than the fee of the target transaction. When an attacker detects a transaction with a large transaction size, he or she submits a counter order to take advantage of the high slippage that temporarily occurs upon the execution of the transaction.

### *4.2. Structural Vulnerabilities in DEX*

The previous chapter described structural attack vulnerabilities caused by MEV characteristics during the block creation process of blockchain. In this chapter, we check the structural vulnerabilities of DEX and various vulnerabilities and attacks caused by services introduced by DEX. Most decentralized exchanges based on AMM are operated as liquidity pools by liquidity providers. A representative attack technique based on this liquidity is the JIT (Just-In-Time) liquidity attack. JIT (hereinafter referred to as 'JIT') attack includes both front-running and back-running and is sometimes called LP (Liquidity Pool) sandwich attack but is referred to as JIT in this paper. Unlike typical sandwich attacks, JIT performs attacks that add and remove liquidity. Intuitively, JIT detects a user's transaction and then adds and removes liquidity before and after it. If you observe this in more detail, it is as shown in Figure 4. Figure 4 assumes the change in liquidity in a single transaction.

To explain JIT with a simple example, the JIT executor acts as a liquidity provider and observes large-scale swap transactions. At this time, the attacker supplies a large amount of liquidity to account for 90% of the supply to the liquidity pool through the front-running method. When a large swap transaction is performed, the transaction fee is paid to the JIT attacker, and liquidity is withdrawn immediately after the transaction. In a JIT attack, only a certain number of bots exist in the network. Most JIT attack attempts occurred at a small number of addresses (0xa57bd00134b2850b2a1c55860c9e9ea100fdd6cf, 0x57c1e0c2adf6eecdb135bcf9ec5f23b319be2c94, etc.). In addition, although this is a type

of attack made easier by the concentrated liquidity added in Uniswap V3, it has the characteristic of requiring attackers to mobilize assets on average 269 times that of users' transactions, and shows low profitability [21].

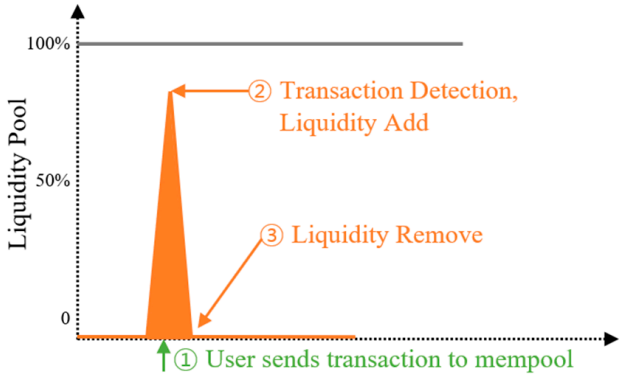



**Figure 4.** Execution process and profit generation section of Just-In-Time Liquidity.

MEV-bot's activities that occur on DEX include an arbitrage strategy that utilizes price differences between various distributed exchanges. Price differences between decentralized exchanges mainly occur when assets have low liquidity or when market information is updated slowly. Arbitrage bots monitor prices on multiple exchanges in real time and achieve profits by purchasing assets at a low price on one exchange and selling them at a high price on another exchange. This process can be considered to contribute to increasing market efficiency and balancing prices between exchanges. However, it can be defined as a type of attack that ultimately causes damage to users and liquidity providers and generates profits. Arbitrage bots can perform arbitrage through their own assets, but more cases of attacks are being discovered through flash loan [22], which was introduced in Uniswap V2. Figure 5 shows the process of conducting arbitrage through flash loans.

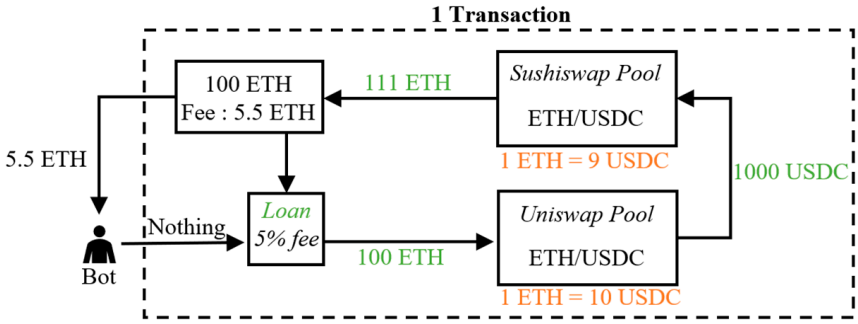



**Figure 5.** DEX flash loan-based arbitrage trading.

Flash loan is a loan method in which you borrow the desired amount of tokens from the pool, use them for the desired task, and then repay the amount and interest within one transaction. Unlike loans in general finance, flash loans do not require collateral or credit, and unlimited loans are possible as long as repayment and fee payment are possible within one transaction through transaction simulation before executing the loan transaction. In Figure 5, arbitrage using flash loans is performed on transactions that achieve the minimum gain, including fee payment, through the price gap between exchanges. There are many examples of attacks such as arbitrage trading using flash loans, start-up manipulation that manipulates the price of the liquidity pool, and protocol hacking. Flash loan and flash swap have been mentioned a lot as the main means of DeFi hacking cases that have continued to occur recently, and negative public opinion has formed. However, the DeFi community, including the Uniswap team, is of the position that the problem is that these functions were abused and used for attacks, and there is no problem with the functions themselves.

## 5. Decentralized Exchange Transaction Analysis

In this section, we work to identify attacks on real DeFi environments and DEXs. For this task, transaction data is collected and analyzed in various ways. The analysis method seeks to determine the number of attacks corresponding to each attack type and identify attack patterns according to trends and issues.

### *5.1. DEX Transaction Data Collection*

We use Dune [23] data table, Etherscan explorer API [24], Transpose custom query API [25], and Etherscan CSV export tool [26] to collect data about decentralized exchanges on the Ethereum blockchain network. Data collection was conducted from January 2022 to December 2023, ranging from a minimum of block number 13,916,330 to a maximum of block number 18,901,697. Figure 6 shows the data collection and analysis steps for the analysis process of this paper.

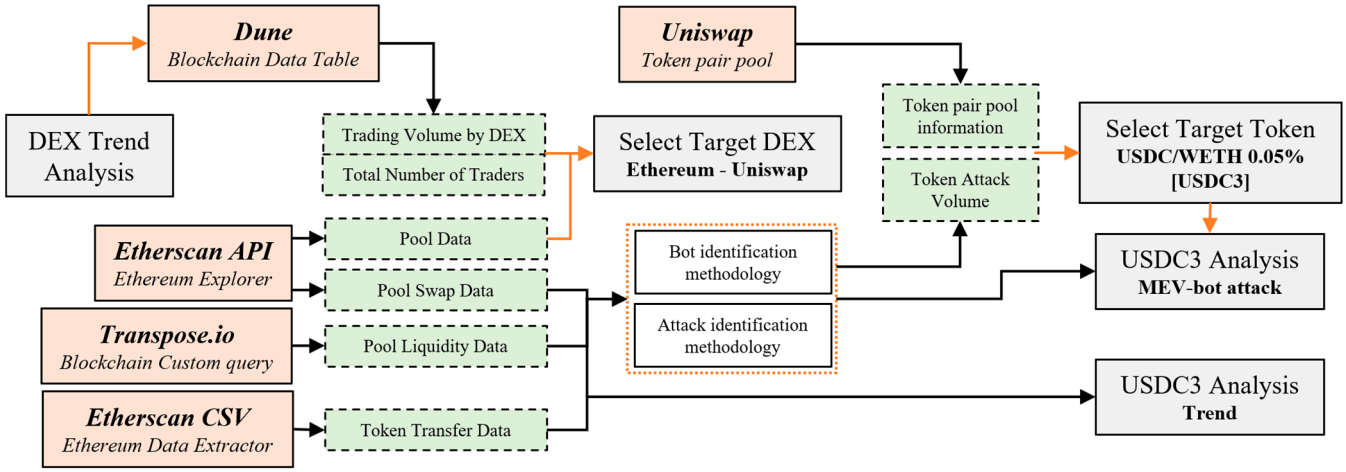



**Figure 6.** Data collection and analysis process for DEX analysis.

Before analyzing attacks occurring on the DEX, we collected the overall data from the DEX to determine which data from which blockchain to collect. According to the blockchain data table provided by Dune, the trading volume of decentralized exchanges from January 2023 to January 2024 reached USD 889 billion, and the number of unique trading accounts during the entire period was confirmed to be about 43.2 million. In this period, the share of blockchain DEX is Ethereum 55%, BNB 18%, and Arbitrum 15%, showing that Ethereum-based DEX is overwhelmingly popular. In the comparison of trading volume between DEXs in Figure 7a, Ethereum-based Uniswap shows overwhelming trading volume.

### *5.2. Identifying MEV-Bot in Transactions*

Attacks by MEV-bot are measured against the USDC/WETH 0.05% token pair pool (0x88e6A0c2dDD26FEEb64F039a2c41296FcB3f5640), which is the token pair pool that is most traded and exposed to the most attacks on Uniswap, an Ethereum-based DEX. To achieve this, we measure bot transactions according to the bot identification methodology below, along with a list of widely known bots provided by Etherscan and Dune. Addresses flagged by three or more of the methods below are classified as bots.

- More than 50 transactions per hour from a specific address;
- More than 100 transactions per 7 days from a specific address;
- More than 80% of transactions in a specific address where the transaction amount per 7 days does not fall to an integer (does not end with *.00USD);
- At least one transaction per hour on the same day from a specific address;
- More than 3 transactions submitted within 10 min after a price change of more than 5% at a specific address.

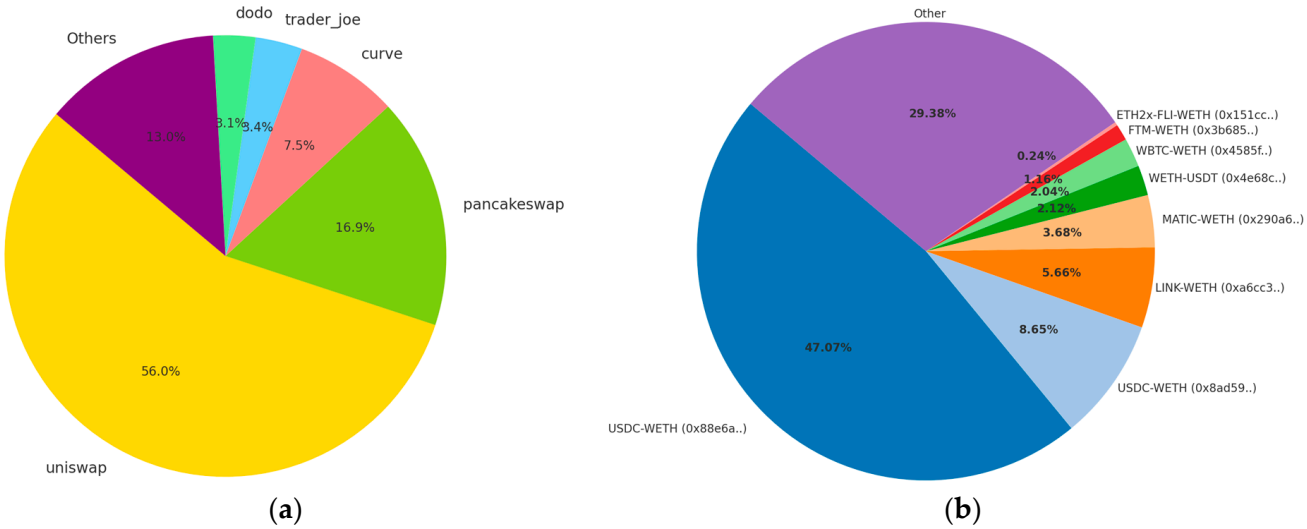



**Figure 7.** (**a**) Pie chart according to transaction share of decentralized exchanges; (**b**) number of attacks on Uniswap's token pairs.

The flow chart in Figure 8 shows how to determine the address of the MEV-bot through the DEX transaction record described above. In addition to the above method, the bot list was confirmed through the confirmed bot account list provided by Etherscan and Dune.

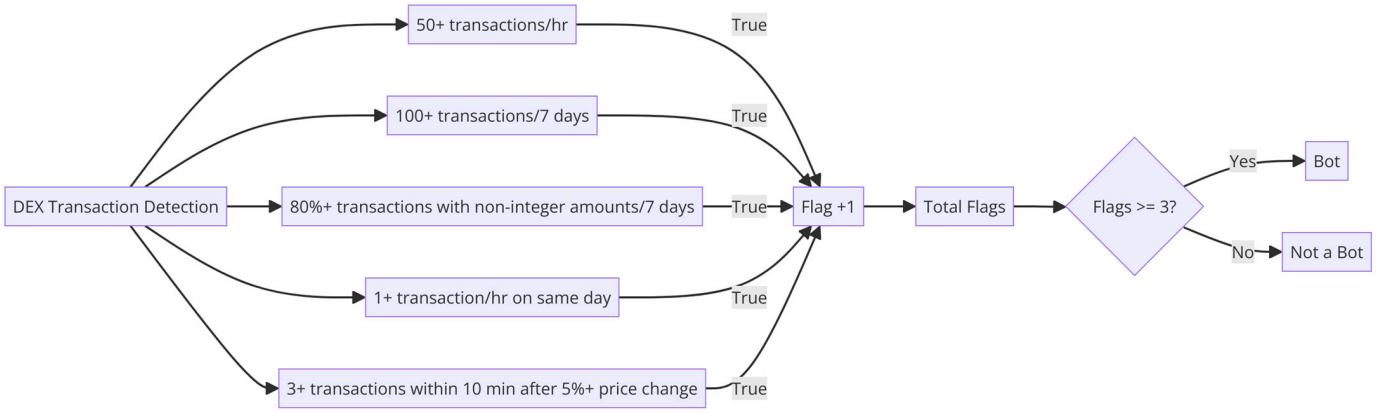
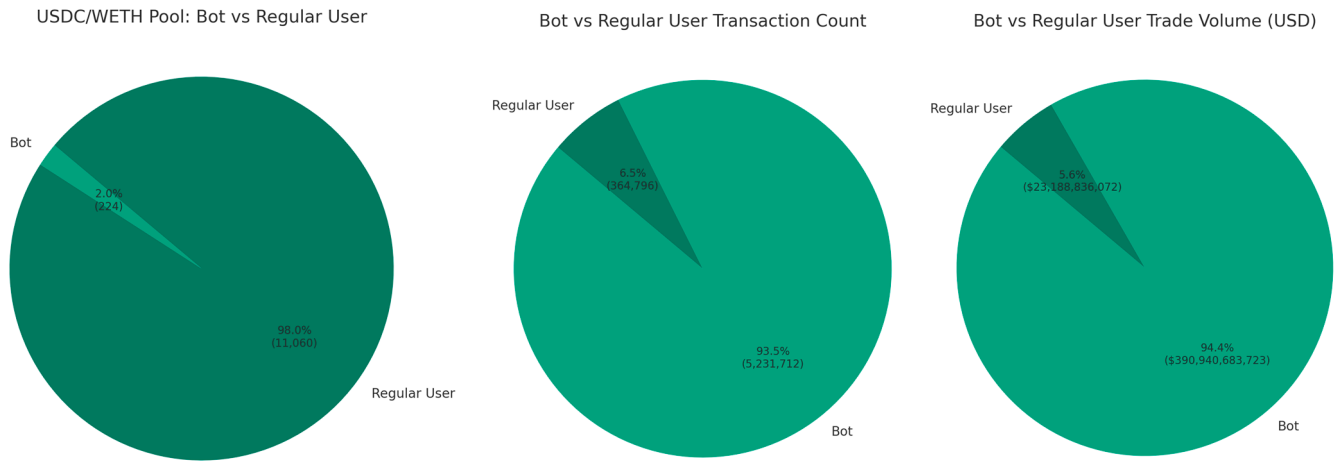



**Figure 8.** Flowchart of methodology for MEV-bot identification in DEX transactions.

Figure 9 is a pie chart graph examining bots and regular users in the USDC/WETH 0.05% pool according to the bot measurement methodology. Through the graph, you can see that automated script accounts, including the MEV-bot service, which accounts for only about 2%, account for about 90% of pool transactions.

Through the previous analysis, we decided to collect transaction data for the USDC/WETH 0.05% token pair pool of Uniswap, a decentralized exchange on the Ethereum blockchain network (0x88e6A0c2dDD26FEEb64F039a2c41296FcB3f5640: USDC3, USDC: 0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48, WETH: 0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2). Table 2 shows the main data collected for analysis.

Through the collected data, we measured the transactions of USDC3 pool bots and regular users over time. Figure 10 shows the number of transactions and volume over time for the two groups in the USDC3 pool. As can be seen in Figure 10b, the volume of MEV-bot attacks rises significantly in situations of large-scale adverse events such as the Terra/Luna plunge, FTX bankruptcy, and Silicon Valley Bank bankruptcy.

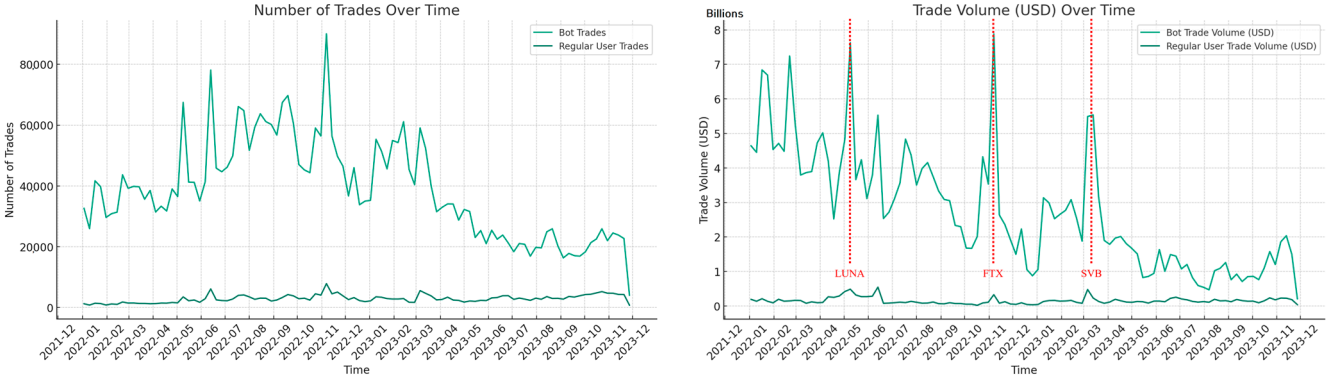



(**a**) (**b**) (**c**)

**Figure 9.** USDC/WETH 0.05% token pair pool analysis until December 2023: (**a**) unique account comparison pie chart of USDC/WETH token pair pool; (**b**) number of transactions in USDC/WETH token pair pool; and (**c**) USD trading volume of USDC/WETH token pair pool.

**Table 2.** Data details based on transaction data collection method.

| Method | Data | Detailed Data | Description |
|---|---|---|---|
| EtherscanAPI | blockNumber | | Number of block in Ethereum Mainnet |
| | timeStamp | | Timestamp |
| | transactionHash | | Transaction Hash |
| | Sender | | Sender address |
| | To | | Receiver address |
| | Data[] | [amount0] | Delta of the token0 balance in the pool |
| | | [amount1] | Delta of token1 balance in pool |
| | | [sqrtPriceX96] | sqrt (price) of pool after swap, Q64.96 |
| | | [liquidity] | Liquidity of pool after swap |
| | | [tick] | Logarithmic base of full price after swap |
| | gasPrice | | Gas price (gwei) |
| | gasUsed | | Used gas in transaction |
| TransposeAPI Custom query | block_number | | Number of block |
| | category | | Type of transaction (e.g., deposit, withdraw) |
| | contract_address | | USDC/WETH:0.05% (0x88...) |
| | contract_version | | Uniswap V3 |
| | exchange_name | | Uniswap |
| | liquidity | | Liquidity of the pool |
| | liquidity_delta | | Change in liquidity |
| | pool_balance | | Pool balance |
| | quantity | | The amount moved in the transaction |
| | sender_address | | Sender address |
| EtherscanCSV Extractor ERC-20 | Txhash | | Transaction hash |
| | Blockno | | Block number |
| | UnixTimestamp | | Unix timestamp |
| | From | | Token sender |
| | To | | Token receiver |
| | TokenValue | | Token value (x ETH, y USDC) |
| | ContractAddress | | USDC/WETH |
| | TokenName | | USDC/wrapped Ethereum |




(**a**) (**b**)

**Figure 10.** USDC/WETH 0.05% token pair pool analysis until December 2023: (**a**) number of transactions over time for USDC/WETH token pair pool and (**b**) USD trading volume over time for the USDC/WETH token pair pool.

MEV-bot attacks are carried out by detecting large-scale transactions by users, and the reason why the bot's transaction volume has increased significantly is because the transactions of general users have also increased proportionately. To interpret the reason why general users' transactions increased on the date indicated by the red dotted line in Figure 10a, it can be predicted as follows:

- LUNA [27]: due to the collapse of stablecoins Terra/Luna, the trust in stablecoins among general users has decreased, leading to a significant increase in the number of users wishing to exchange USDC for WETH, and resulting in an increase in MEV-bot activity;
- FTX [28]: the bankruptcy of FTX, a large centralized cryptocurrency exchange, led to a surge in demand for decentralized exchanges, resulting in increased trading volume and increased MEV-bot activity;
- SVB: the bankruptcy of Silicon Valley Bank, a centralized financial bank, led to a surge in demand for cryptocurrency and a surge in demand for decentralized exchanges, leading to an increase in MEV-bot activity.

In this way, decentralized exchanges tend to couple from general centralized finance. As governments and institutions immediately announce policies to support the bankruptcy and instability of centralized exchanges, we can see a decrease in trading volume. However, as the crisis of centralized exchanges repeats, the number of users choosing DEX and DeFi is increasing.

### *5.3. Transaction Analysis according to DEX Attack Type*

A large number of MEV-bots are being serviced and active on the DEX service platform. In order to understand and analyze the environment of decentralized finance, we detected and analyzed several attack methods introduced earlier based on collected transaction data. First, to analyze sandwich attacks, we present standards for classifying sandwich bots and attacks from transaction data. The attacker identification criteria are as follows:

1. Transactions tx1, tx2 of the same account performed within the same block;
2. Both tx1 and tx2 for swap are performed within the same block;
3. Tokens purchased in tx1 and tokens sold in tx2 are the same; tokens sold in tx1 and tokens purchased in tx2 are the same to include rare but opposite cases;
4. The amount of token purchase in Tx1 and the amount of token sale in tx2 are the same;
5. The amount of tokens sold to Tx1 is less than the amount of tokens purchased from tx2 (the sandwich attacker attempted a sandwich attack but suffered a loss).

The volume of identified sandwich attacks reaches USD 21.2 billion in 2023, with an average attack volume of about USD 40,000, and USD 139.2 billion in the period from

January 2022 to the present (volume for an attack refers to the volume used for the attack, not the bot's benefit). The daily average of sandwich bot transactions is approximately 4000, accounting for approximately 8% of transactions in the pool. In addition, the fee (gas) paid by Sandwich Bot reaches an average of 2100 ETH per month, and the fee paid in transactions is about 30% more than that of regular users. This is confirmed to be a phenomenon that occurs when high priority transactions are submitted for front-running. The sandwich bot's revenue is defined by Equations (2) and (3), but an attack is only attempted if this revenue is higher than the gas fee. Accordingly, as shown in Figure 11, a correlation between the Ethereum network fee cost and the type of sandwich bot attack is observed. Gas fees for Ethereum 2.0, which completed the merge in 2022 and converted to PoS, are gradually decreasing, and as a result, the attack range of sandwich bots is expanding [29]. The scope for users to suffer losses when conducting token swap transactions on DEX is expanding.

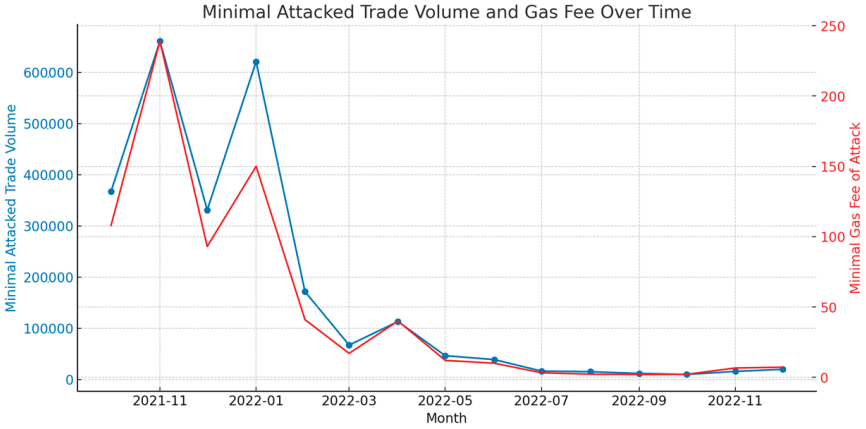



**Figure 11.** Correlation between 'Minimum Attacked Transaction Volume' and 'Minimum Attacked Gas Fee' for Ethereum USDC3 over 15 months from October 2021 to December 2022.

JIT, another front-running-based attack technique, creates and simultaneously burns liquidity positions within the same block. The JIT attacker's profits are the fees of users who performed large-scale transactions while creating liquidity positions, and they generate profits by intercepting the fees of existing liquidity providers. The liquidity temporarily provided by JIT attackers averages USD 17 million, and the average victim's swap volume is USD 140,000. Unlike sandwich attacks, JIT attacks do not cause any damage on the surface to the user. However, it is an attack that damages and steals the fees of existing liquidity providers who supply liquidity to the pool, and there is a risk of destroying the soundness of Token Fairpool. JIT attackers accounted for USD 740 billion of the USD 760 billion in liquidity trading volume in the USDC3 pool across the top 25 accounts. Even when narrowing down to the top five accounts, the liquidity accounted for was USD 300 billion. JIT attackers form a market with small but very large assets.

An arbitrage bot is a series of two or more transactions occurring in the same transaction, where the first token purchased (token_in) is the same as the last token sold in the transaction (token_out). In other words, in a single transaction, it is a transaction that satisfies amount (token_in = token_out) and price (token_in < token_out) regardless of transaction DEX. In the case of arbitrage bots, they accounted for approximately 32% of MEV-bot activity volume over the entire period, generating an average of 12,000 transactions per day. Like the previous incident, arbitrage bots generate profits based on slippage generated by price differences between exchanges. Figure 12 is a graph showing the transactions and attack activities of arbitrage bots in 2023. Due to the Silicon Valley Bank bankruptcy that occurred in March 2023, a large amount of physical assets flowed into the cryptocurrency market, and the activity of arbitrage bots increased due to slippage between exchanges that occurred as the inflow investors purchased cryptocurrency.

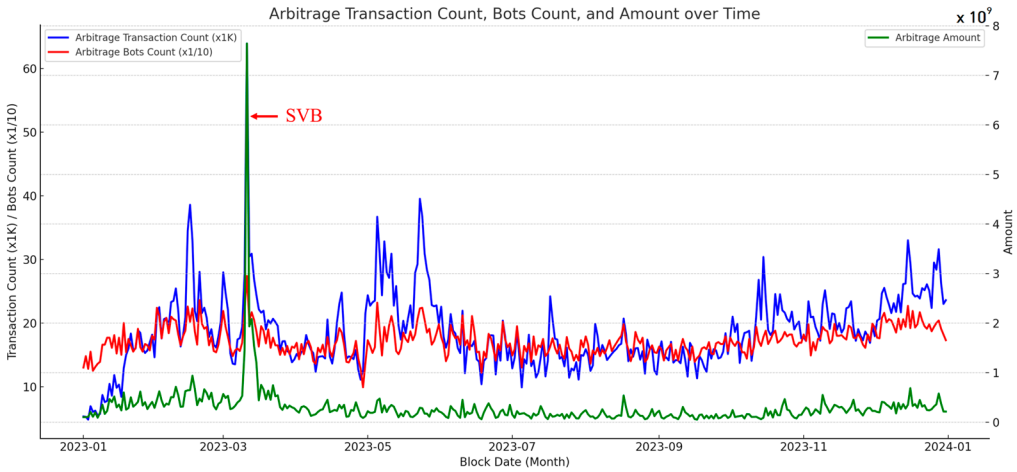



**Figure 12.** Transaction and attack volume of arbitrage bots in 2023.

Figure 13 is a graph of the liquidity events and pool balance of the Uniswap USDC/WETH token pair pool, and the spot price of Ethereum coins. Figure 13 shows the Luna crash and FTX bankruptcy events. This event is bad news for the blockchain, and as a result, the price of Ethereum spot assets fell. However, as the price of Ethereum falls and the subsequent fee price falls, decentralized finance shows an upward trend in the graph. This trend may be due to the decline in the price of ETH and the large amount of token swaps that occurred due to the stable characteristics of USDC. Large-scale transactions where WETH is swapped for USDC are increasing, and this increase in DEX trading volume increases the number of liquidity providers targeting fees for providing liquidity. Accordingly, in Figure 13, the pool balance and swap amount increased significantly.

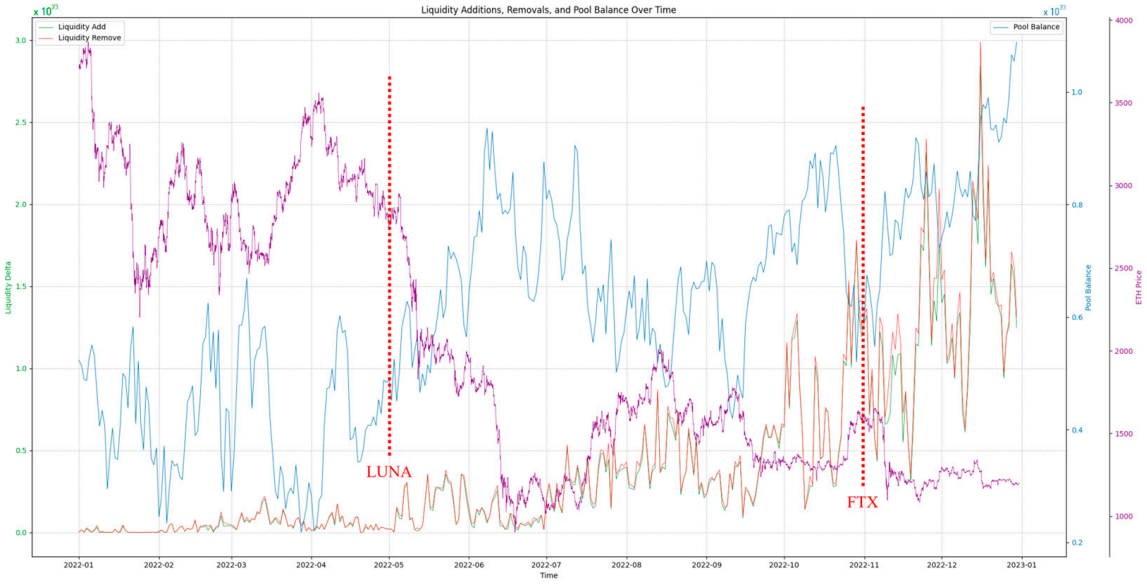



**Figure 13.** Graph of Uniswap USDC/WETH Token Fairpool liquidity events and pool balance and Ethereum price.

As can be seen in Figures 10, 12 and 13, the cryptocurrency market is characterized by large fluctuations in market value due to financial issues such as the Luna crash and the FTX bankruptcy. What we watched most closely was when assets from the centralized financial market flowed into the cryptocurrency market due to SVB's bankruptcy, and after dollars were exchanged for cryptocurrency, exchange between assets took place through DEX. Several MEV-bots generate the greatest activity and profits during times when these large

transactions are detected. The Uniswap team and community claim that these MEV-bot activities are legitimate economic activities, but there is a need to sanction the activities of MEV-bots for the reliability of blockchain technology, decentralized finance, and fair trading on exchanges. When users trade in the decentralized market, the risk of asset theft and reckless bot activity are barriers to market entry and will become obstacles to technological development. There is a need to research safe and fair transaction technology for DEX transactions, and measures to protect general users even in a decentralized environment are urgently needed.

## 6. Discussion and Conclusions

The patterns and vulnerabilities revealed through transaction analysis and bot detection not only highlight the vulnerability of DeFi systems to MEV attacks but also highlight the urgent need for adaptive security strategies. Additionally, proposals for advanced monitoring systems to detect and respond to MEV attacks could lead to a more proactive approach to DeFi security. DeFi platforms can integrate sophisticated monitoring tools to identify and mitigate attacks at an early stage, thereby maintaining transaction accuracy, market dynamics, and user trust. Another important aspect of our research is our focus on developing transaction technologies that ensure fairness in a decentralized environment. This is especially important to maintain the ethics of decentralization: fairness and transparency. The deployment of these technologies could revolutionize DeFi transactions, making them fairer and more resistant to manipulation. In conclusion, our study contributes significantly to the ongoing discourse on enhancing DeFi security. The potential applications of our findings are vast, extending from immediate improvements to existing DeFi platforms to guiding the development of future blockchain technologies. By continuing to study these evolving threats, we can build stronger and safer financial structures in the decentralized finance space and ensure sustainable growth and widespread adoption of these innovative platforms.

This paper focuses on decentralized exchanges, especially Uniswap, and highlights a significant risk in the field of decentralized finance (DeFi) called Maximal Extractable Value (MEV) attacks. Our extensive transaction analysis and bot detection methods were instrumental in identifying and understanding the patterns of these attacks. This study reveals the complex structure of the DeFi ecosystem and its vulnerability to sophisticated threats such as MEV-bots. These attacks have a significant impact not only on the accuracy of transactions but also on market dynamics and trust in the overall DeFi system. The correlation between events and MEV attacks on blockchain and financial markets suggests that attackers are taking advantage of market volatility and network congestion.

Based on these findings, this paper emphasizes the need for sustainable economics and adaptive security strategies in DeFi. We support the deployment of more dynamic security protocols and advanced monitoring systems to proactively detect and respond to MEV attacks. Additionally, we urge the development of transaction technology for fair transactions in a decentralized environment. This study paves the way for further research into the evolving nature of these threats and the development of more robust financial structures within the decentralized space. In conclusion, DeFi and DEX are revolutionizing financial services, but their security remains a critical issue. This study highlights the need for research to enhance the safety and reliability of these platforms.

**Author Contributions:** Conceptualization, H.K.; Methodology, N.C.; Software, N.C.; Writing—original draft, N.C.; Writing—review & editing, H.K.; Project administration, H.K. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by Kyonggi University Research Grant 2021.

**Data Availability Statement:** Data are contained within the article.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References


1. Schär, F. Decentralized Finance: On Blockchain-and Smart Contract-Based Financial Markets. *FRB St. Louis Rev.* **2021**, *103*, 153–174. [CrossRef]
2. Popescu, A.D. Understanding FinTech and Decentralized Finance (DeFi) for Financial Inclusion. In *FinTech Development for Financial Inclusiveness*; IGI Global: Hershey, PA, USA, 2022; pp. 1–13, ISBN 978-1-79988-447-7. [CrossRef]
3. Wu, S.; Wang, D.; He, J.; Zhou, Y.; Wu, L.; Yuan, X.; He, Q.; Ren, K. DeFiRanger: Detecting Price Manipulation Attacks on DeFi Applications. *arXiv* **2021**. [CrossRef]
4. Heimbach, L.; Wattenhofer, R. SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance. In Proceedings of the 4th ACM Conference on Advances in Financial Technologies, Cambridge, MA, USA, 19–21 September 2022; pp. 47–60. [CrossRef]
5. Zhou, L.; Qin, K.; Torres, C.F.; Le, D.V.; Gervais, A. High-Frequency Trading on Decentralized On-Chain Exchanges. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24–27 May 2021; pp. 428–445. [CrossRef]
6. Alam, T.; Ali, M.; Rahman, M. Front-Running Attack in Decentralized Finance in the Metaverse: A Systematic Review. *Int. J. Sci. Res. Arch.* **2024**, *11*, 2315–2324. [CrossRef]
7. Xiang, D.; Lin, Y.; Nie, L.; Zheng, Y.; Xu, Z.; Ding, Z.; Liu, Y. An Empirical Study of Attack-Related Events in DeFi Projects Development. *Empir. Softw. Eng.* **2024**, *29*, 49. [CrossRef]
8. Arora, S.; Li, Y.; Feng, Y.; Xu, J. SecPLF: Secure Protocols for Loanable Funds against Oracle Manipulation Attacks. *arXiv* **2024**, arXiv:2401.08520.
9. Huang, K.; Chen, X.; Yang, Y.; Ponnapalli, J.; Huang, G. ChatGPT in Finance and Banking. In *Beyond AI: ChatGPT, Web3, and the Business Landscape of Tomorrow*; Huang, K., Wang, Y., Zhu, F., Chen, X., Xing, C., Eds.; Future of Business and Finance; Springer Nature Switzerland: Cham, Switzerland, 2023; pp. 187–218, ISBN 978-3-031-45282-6.
10. Parhizkari, B.; Iannillo, A.K.; Ferreira Torres, C.; Banescu, S.; Xu, J. Timely Identification of Victim Addresses in DeFi Attacks. In Proceedings of the International Workshop on Cryptocurrencies and Blockchain Technology (CBT), The Hague, The Netherlands, 25–29 September 2023; Springer: Cham, Switzerland, 2023.
11. Chaliasos, S.; Charalambous, M.A.; Zhou, L.; Galanopoulou, R.; Gervais, A.; Mitropoulos, D.; Livshits, B. Smart Contract and DeFi Security Tools: Do They Meet the Needs of Practitioners? In Proceedings of the Proceedings of the 46th IEEE/ACM International Conference on Software Engineering, Lisbon, Portugal, 14–20 April 2024; Association for Computing Machinery: New York, NY, USA, 2024; pp. 1–13.
12. Kaur, G.; Habibi Lashkari, A.; Sharafaldin, I.; Habibi Lashkari, Z. *Understanding Cybersecurity Management in Decentralized Finance: Challenges, Strategies, and Trends*; Financial Innovation and Technology; Springer International Publishing: Cham, Switzerland, 2023; ISBN 978-3-031-23339-5.
13. Krishnamurthi, R.; Shree, T. A Brief Analysis of Blockchain Algorithms and Its Challenges. In *Architectures and Frameworks for Developing and Applying Blockchain Technology*; IGI Global: Hershey, PA, USA, 2019; pp. 69–85, ISBN 978-1-5225-9257-0. [CrossRef]
14. Introducing Uniswap V3. Available online: https://blog.uniswap.org/uniswap-v3 (accessed on 31 January 2024).
15. Wu, M.; McTighe, W. Constant Power Root Market Makers. *arXiv* **2022**, arXiv:2205.07452.
16. Wang, Y.; Chen, Y.; Wu, H.; Zhou, L.; Deng, S.; Wattenhofer, R. Cyclic Arbitrage in Decentralized Exchanges. In Proceedings of the Companion Proceedings of the Web Conference 2022, Lyon, France, 25–29 April 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 12–19. [CrossRef]
17. Fábregas, J. Tracking Ethereum Blockchain Crypto Attackers: Measuring Sandwich Attacks. Available online: https://www.tarlogic.com/blog/ethereum-blockchain-sandwich-attacks/ (accessed on 1 December 2023).
18. Daian, P.; Goldfeder, S.; Kell, T.; Li, Y.; Zhao, X.; Bentov, I.; Breidenbach, L.; Juels, A. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. *arXiv* **2019**. [CrossRef]
19. Uniswap/Universal-Router. Available online: https://github.com/Uniswap/universal-router (accessed on 31 January 2024).
20. Welcome to Flashbots | Flashbots Docs. Available online: https://docs.flashbots.net/ (accessed on 31 January 2024).
21. Xiong, X.; Wang, Z.; Knottenbelt, W.; Huth, M. Demystifying Just-in-Time (JIT) Liquidity Attacks on Uniswap V3. In Proceedings of the 2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 11–13 October 2023. Cryptology ePrint Archive 2023.
22. Flashloans. Available online: https://flashloans.com/ (accessed on 31 January 2024).
23. Dune—Crypto Analytics Powered by Community. Available online: https://dune.com/home (accessed on 31 January 2024).
24. Introduction of Etherscan API. Available online: https://docs.etherscan.io/ (accessed on 31 January 2024).
25. Transpose. Available online: https://www.transpose.io/ (accessed on 31 January 2024).
26. Etherscan Export CSV Data. Available online: https://etherscan.io/exportData (accessed on 31 January 2024).
27. Briola, A.; Vidal-Tomás, D.; Wang, Y.; Aste, T. Anatomy of a Stablecoin's Failure: The Terra-Luna Case. *Financ. Res. Lett.* **2023**, *51*, 103358. [CrossRef]

28. Vidal-Tomás, D.; Briola, A.; Aste, T. FTX's Downfall and Binance's Consolidation: The Fragility of Centralised Digital Finance. *Phys. A Stat. Mech. Its Appl.* **2023**, *625*, 129044. [CrossRef]
29. Kapengut, E.; Mizrach, B. An Event Study of the Ethereum Transition to Proof-of-Stake. *Commodities* **2023**, *2*, 96–110. [CrossRef]