Security of Critical Infrastructure in Decentralized Finance (DeFi)

Sanidhay Arora*
sanidhay@uoregon.edu
University of Oregon
Eugene, OR, USA

ABSTRACT

Decentralized Finance (DeFi) has revolutionized the financial landscape by providing open, permissionless, and decentralized alternatives to traditional financial systems. However, the rapid growth of DeFi has also exposed significant risks, particularly within its critical infrastructure—Decentralized Exchanges (DEXs) and Protocols for Loanable Funds (PLFs). This work presents a comprehensive risk analysis survey focusing on the protocol layer (PL) and smart contract (SCL) layer. We examine the underlying mechanisms, vulnerabilities, and threat vectors inherent to DEXs and PLFs. We provide a structured approach to identifying, assessing, and mitigating risks. This survey integrates technical, economic, and governance perspectives, offering a holistic view of risk management in DeFi. We propose practical guidelines and methodologies for enhancing the security and resilience of the critical infrastructure of DeFi, thereby fostering a more stable and reliable ecosystem.

KEYWORDS

Blockchain, Decentralized Finance (DeFi), smart contract vulnerability

1 INTRODUCTION

Decentralized Finance (DeFi) [1–65] has emerged as a groundbreaking innovation in the financial sector, characterized by its reliance on blockchain technology to orchestrate financial services without centralized intermediaries. This paradigm shift not only democratizes financial services but also introduces a complex landscape of security challenges that are intrinsic to its decentralized nature.

This paper makes the following contributions:

- Risk Analysis Survey: A comprehensive risk analysis survey specifically focused on the characteristics of DeFi's critical infrastructure, i.e. focusing on Decentralized Exchanges (DEXs) and Protocols for Loanable Funds (PLFs).
- Protocol Layer Analysis: Detailed examination of the protocol design layer, identifying key vulnerabilities, potential attacks, and mitigation strategies. This includes analysis of consensus mechanisms, governance models, and protocol upgrades.
- Smart Contract Layer Analysis: Investigation of the smart contract layer, highlighting common security flaws, auditing practices, and techniques to enhance contract robustness. This encompasses issues such as reentrancy attacks, oracle manipulations, and flash loan exploits.
- Technical Perspective: Taxonomy of technical aspects, including interoperability standards, and decentralized oracles, to understand their impact on the security and functionality of DEXs and PLFs.
- Economic Perspective: Assessment of economic risks, such as market manipulation, liquidity risks, and incentive misalignments, providing insights into how these factors influence the stability of DeFi protocols.
- Governance Perspective: Analysis of governance-related risks, including decentralized governance structures, decision-making processes, and community-driven protocol changes, to understand their role in risk management and resilience.
- Risk scoring model: A risk scoring model using risk matrix and Failure Mode and Effect Analysis (FMEA) to quantify the severity and likelihood of risk. This model considers the analysis from the three aforementioned perspectives.

2 RELATED WORK

The rapidly growing field of Decentralized Finance (DeFi) has garnered significant academic and industry attention due to its decentralized nature and unique financial opportunities. However, this innovation comes with many security challenges. In this section, we compare the contributions of different surveys and studies on DeFi, highlighting their focus areas and how they relate to the current work.

Security Challenges in DeFi. Li et al. [32] provide an in-depth examination of the security risks in DeFi, categorizing them into technical, economic, and governance-related vulnerabilities. Their work emphasizes smart contract vulnerabilities such as reentrancy attacks, flash loan exploits, and price oracle manipulations, while also addressing governance-related risks like voting power concentration in decentralized autonomous organizations (DAOs). This work forms the basis of core DeFi vulnerabilities; however, it does not provide a systematic risk assessment model. In our work, we aim to quantify both the likelihood and impact of risks.

Smart Contract Vulnerabilities. Ivanov et al. [26] focus specifically on smart contract security, analyzing common flaws in DeFi platforms. They identify the most frequent smart contract vulnerabilities, including integer overflows, reentrancy issues, and improper access controls. While Ivanov et al. provide a valuable taxonomy of technical risks, their work lacks a broader perspective on how these vulnerabilities affect the protocol and governance layers of DeFi. Our work expands on this by integrating technical, economic, and governance aspects into a unified risk analysis.

Risk Mitigation Strategies. Baum et al. [4] propose various methods to mitigate front-running attacks and related vulnerabilities in DeFi applications. They focus primarily on technical solutions like timelocks and multi-signature wallets to secure smart contract operations. While their work provides valuable technical guidelines, our survey expands these strategies to cover the protocol and governance layers, where additional risks like governance exploits and unsafe dependencies can affect the overall security of DeFi platforms

*

Systemic Risks in DeFi. Bekemeier's [5] analysis addresses the systemic risks in DeFi by exploring how vulnerabilities in interconnected protocols can lead to cascading failures across the ecosystem. This study highlights the importance of addressing both individual protocol risks and the broader implications of liquidity crises and governance manipulation. Our work builds on this by introducing a risk scoring model that evaluates both the severity and likelihood of potential attacks, providing developers and policymakers with actionable insights for preventing systemic failures focusing on the Critical Infrastructure of DeFi.

Governance Attacks. Several works have highlighted the risks posed by decentralized governance mechanisms in DeFi. Chitra and Kulkarni [14] investigate how governance tokens can be manipulated by acquiring significant voting power, allowing attackers to pass malicious proposals. This is a critical concern in the growing DeFi landscape, where governance structures play a pivotal role in managing protocol upgrades and decisions. Our survey not only addresses these governance-related vulnerabilities but also offers practical guidelines for improving decision-making processes in decentralized platforms.

Despite the growing body of literature on DeFi security, several gaps remain in the existing research. One of the critical areas is the systemization of various attack types, their risk levels, and the solutions currently available. There is a need to classify attacks not only by their technical difficulty but also by the likelihood of occurrence, which depends on both technical and economic factors. Additionally, many state-of-the-art solutions are limited in scope [20, 21]. These works only address specific types of vulnerabilities without providing a holistic view of risk management across the DeFi ecosystem. This survey aims to bridge these gaps by providing a structured approach to identifying, assessing, and mitigating risks, particularly in the protocol and smart contract layers of decentralized exchanges (DEXs) and protocols for loanable funds (PLFs).

In summary, existing surveys and research have provided invaluable insights into specific areas of DeFi security, focusing primarily on smart contract vulnerabilities, MEV, and governance-related risks. However, a comprehensive model that addresses the full spectrum of risks—spanning technical, economic, and governance factors—is still lacking. Our work aims to fill this gap by offering a structured risk analysis that integrates multiple perspectives and provides practical guidelines for enhancing the security and resilience of Critical Infrastructure of DeFi.

3 BACKGROUND

The following references provide a background on DeFi, including preliminaries like applications and their architecture and design mechanism; security risks and vulnerabilities; and summarizes the surveys and SoKs in various aspects of DeFi [4, 22, 44, 57, 59, 65].

Overview of critical infrastructure. DeFi's critical infrastructure comprises various protocols and platforms that facilitate decentralized financial transactions. Among these, Decentralized Exchanges (DEXs) and Protocols for Loanable Funds (PLFs) are fundamental.

- **Decentralized Exchanges (DEXs)**: DEXs enable users to trade digital assets directly with one another without the need for a central intermediary. These exchanges operate through smart contracts that automate transactions, providing greater transparency and security compared to traditional exchanges. Common examples include Uniswap, SushiSwap, and Curve.
- **Protocols for Loanable Funds (PLFs)**: PLFs allow users to lend and borrow digital assets in a decentralized manner. These protocols use smart contracts to facilitate loans, calculate interest rates, and manage collateral. Major examples include Aave, Compound, and MakerDAO.

Both DEXs and PLFs have experienced significant growth and adoption, driven by their ability to offer innovative financial services. However, their complexity and the high value of assets involved make them prime targets for various risks.

Preliminaries. The foundation of Decentralized Finance (DeFi) lies in its ability to operate financial services without the need for centralized intermediaries. Harvey et al. [24] provide an expansive overview of the future of finance in the context of DeFi, where blockchain technology underpins the decentralized infrastructure. Blockchain security and privacy, as discussed by Karame and Capkun [27], are also crucial pillars in ensuring the smooth operation and trust in DeFi ecosystems. The security risks in DeFi often stem from the unique challenges introduced by the decentralized nature of its operations, especially in managing trust between anonymous participants and external services such as oracles and cross-chain bridges.

DeFi Surveys. Several comprehensive surveys have been conducted to evaluate the security landscape of DeFi. Ivanov et al. [26] provide a broad analysis of smart contract security threats, outlining key vulnerabilities such as reentrancy attacks, integer overflows, and improper access controls. Li et al. [32] focus on the broader security challenges in DeFi, providing a detailed account of the various economic, technical, and governance-related risks that emerge due to the decentralized nature of financial operations. These surveys serve as a critical resource in understanding the array of vulnerabilities that affect the DeFi ecosystem.

Specific Attacks and Vulnerabilities. In-depth studies on DeFi-specific vulnerabilities highlight various attack vectors and their impact on the ecosystem. DeFiRanger [1], for instance, discusses techniques for detecting price manipulation attacks, one of the more common exploits in decentralized exchanges (DEXs). Chitra and Kulkarni's [14] work focuses on the economic risks associated with Miner Extractable Value (MEV) and its relationship to proof-of-stake systems, emphasizing the risks of front-running attacks. Daian et al. [15] further expand on this by exploring front-running attacks in DEXs, where the transparency of blockchain transactions enables attackers to manipulate the order of transactions for financial gain.

Mitigation Strategies. Mitigation strategies for DeFi security risks have evolved in response to the growing complexity and frequency of attacks. Baum et al. [4] offer solutions for front-running mitigation, while Brent et al. propose a security analyzer designed specifically for the Ethereum Virtual Machine (EVM), which powers many DeFi platforms. Another significant concern is the presence of practical centralization risks. Yan et al. [61] show that certain DeFi protocols exhibit centralized control, leading to vulnerabilities that undermine the decentralized ethos of the ecosystem. The solutions

proposed in these works range from technical audits to governance reforms aimed at minimizing the risk of malicious activities.

Economic Impact and System Risks. The economic implications of security vulnerabilities in DeFi extend beyond individual attacks due to systemic consequences. Bekemeier's [5] analysis of systemic risks in decentralized finance explores how interconnected protocols can lead to cascading failures across the ecosystem. Gudgeon et al. [23] study the efficiency of loanable funds protocols in DeFi. They discuss the mechanics of liquidity risks and incentive misalignments and how they lead to both market inefficiencies and significant financial losses. These studies underscore the need for a more robust understanding of the economic dynamics that govern DeFi protocols.

Empirical Studies and Analysis. Empirical research is essential for understanding the real-world behavior and performance of DeFi platforms. Babel et al. [3] present an in-depth analysis of the economic security of smart contracts. They provide quantitative data on the various vulnerabilities that have been exploited in the wild. Chaliasos et al. [10] contribute to this body of work by evaluating tools and practices used by practitioners to secure smart contracts and DeFi platforms. Their empirical studies reveal gaps in current auditing practices and suggest areas for improvement to enhance the resilience of DeFi against attacks.

The purpose of this survey is to provide a structured approach to identifying, assessing, and mitigating risks within the protocol layer and smart contract layer of DEXs and PLFs. The scope includes technical, economic, and governance perspectives to offer a holistic view of risk management.

3.1 Key Components

The key components of the survey are as follows:

- Protocol Layer (PL): Focuses on the structural and operational aspects of the protocols.
- Smart Contract Layer (SCL): Addresses the security and functionality of the smart contracts.
- Technical Factors: Examines the underlying technology and infrastructure.
- Economic Factors: Considers the financial dynamics and market behaviors.
- Governance Factors: Considers the decision-making processes and community involvement.

Protocol Layer (PL) The Protocol Layer (PL) involves the fundamental rules and mechanisms that govern the operation of DEXs and PLFs. This includes consensus algorithms, governance models, and the overall architecture of the protocols.

Smart Contract Layer (SCL). Smart contracts are self-executing contracts with the terms of the agreement directly written into code. In DEXs and PLFs, they automate various processes such as trade execution, loan issuance, and collateral management.

The common auditing practices involved in the smart contract layer defence include:

- Code Reviews: Thorough examination of the smart contract code by experienced auditors.
- Formal Verification: Using mathematical methods to prove the correctness of the smart contracts.
- Bug Bounties: Offering rewards for discovering and reporting vulnerabilities.

Some common techniques to enhance contract robustness include:

- Modular Design: Building contracts in a modular fashion to isolate and contain potential issues.
- Timelocks: Implementing time delays for critical functions to allow for intervention in case of suspicious activity.
- Multi-Signature Wallets: Requiring multiple approvals for significant transactions to reduce the risk of a single point of failure.

Economic Factors. Economic factors play a crucial role in the stability and functionality of Decentralized Finance (DeFi) systems. These factors not only determine the operational dynamics of platforms but also introduce specific vulnerabilities tied to market manipulation, liquidity crises, and incentive misalignments. The major economic factors include the following:

- **Market Manipulation**
  - Pump and Dump Schemes: Coordinated efforts to artificially inflate asset prices.
  - Wash Trading: Creating fake trading volume to mislead investors.
- **Liquidity Risks**
  - Impermanent Loss: Losses incurred by liquidity providers due to price volatility.
  - Liquidity Crises: Situations when there is insufficient liquidity to meet user demands.
- **Incentive Misalignments**
  - Misaligned Rewards: Incentive structures that do not align with long-term protocol health.
  - Governance Manipulation: Economic incentives that encourage malicious governance actions.

Governance Factors. Governance is a central component of Decentralized Finance (DeFi) platforms, dictating how decisions are made, protocols are upgraded, and community input is integrated. Unlike traditional financial systems, DeFi governance relies on decentralized structures, often through token-based voting mechanisms. However, this introduces risks related to governance manipulation. The following are the relevant governance factors:

- **Decentralized Governance Structures**
  - Token-Based Voting: Governance decisions made based on token holdings.
  - Quadratic Voting: A voting system that aims to reduce the influence of large token holders.
- **Decision-Making Processes**
  - Proposals and Voting: How changes to the protocol are proposed and approved.
  - Delegate Systems: Empowering representatives to make decisions on behalf of the community.
- **Community-Driven Protocol Changes**
  - Community Involvement: Encouraging active participation from the user base.
  - Transparency and Accountability: Ensuring governance decisions are transparent and accountable.

Technical Factors. Technical factors are the backbone of Decentralized Finance (DeFi) platforms, encompassing the interoperability standards, and decentralized oracles that power the ecosystem. The reliability and security of these technical components are essential for the smooth operation of DeFi protocols. Vulnerabilities at this level can lead to catastrophic failures, including data breaches and financial losses. The following are the relevant technical factors:

- **Interoperability Standards**
  - Cross-Chain Communication: Protocols that enable interaction between different blockchain networks.
  - Token Standards: Common standards like ERC-20 and ERC-721 that facilitate token compatibility.
- **Decentralized Oracles**
  - Role of Oracles: Providing off-chain data to smart contracts.
  - Security Challenges: Ensuring the accuracy and integrity of Oracle data.
  - Mitigation Strategies: Using multiple oracles and decentralized oracle networks to reduce the risk of manipulation.

4 THREAT MODEL

The threat model considers different adversarial capabilities, ranging from technical expertise and computational resources to financial influence and network manipulation. We assume that an adversary $\mathbb{A}$ is a rational agent aiming to maximize its utility. Adversary $\mathbb{A}$ operates within the DeFi ecosystem, targeting Decentralized Exchanges (DEXs) and Protocols for Loanable Funds (PLFs). The following sections outline the capabilities and knowledge of an adversary $\mathbb{A}$. An adversary possessing all listed capabilities and knowledge is an improbable case. The access to these capabilities and knowledge determines the threat level of the adversary $\mathbb{A}$. This model can be used in developing effective risk management strategies for the critical infrastructure of DeFi.

4.1 Adversarial Capabilities

The following are the capabilities that an Adversary can possess. These capabilities may vary for different adversaries and a single adversary may not possess all of them.

$\mathbb{AC}_1$ **Technical Expertise**: $\mathbb{A}$ possesses a deep understanding of blockchain technology, smart contracts, and the specific protocols used by DEXs and PLFs.

$\mathbb{AC}_2$ **Computational Resources**: $\mathbb{A}$ has access to significant computational power, allowing it to perform complex calculations, execute sophisticated attacks such as 51% attacks, and engage in extensive data analysis.

$\mathbb{AC}_3$ **Financial Resources**: $\mathbb{A}$ can mobilize substantial financial assets, facilitating activities such as flash loan attacks, market manipulation, and liquidity provision to gain undue influence over protocols.

$\mathbb{AC}_4$ **Network Influence**: $\mathbb{A}$ can orchestrate network-level attacks, including Sybil attacks, where multiple fake identities are created to manipulate consensus or governance processes.

$\mathbb{AC}_5$ **Adaptive Strategies**: $\mathbb{A}$ can adapt its strategies in response to the evolving security measures and defenses employed by DeFi platforms. This includes leveraging new vulnerabilities as they are discovered and dynamically adjusting attack methods.

4.2 Adversarial Knowledge

The following summarizes the types of knowledge that an Adversary can possess. Note that a single adversary may not possess all of them.

$\mathbb{AK}_1$ **Protocol Specifications**: $\mathbb{A}$ is well-versed in the technical documentation, whitepapers, and source code of target protocols. This detailed knowledge allows the adversary to understand the inner workings and identify potential design flaws or vulnerabilities.

$\mathbb{AK}_2$ **Network State and Transactions**: $\mathbb{A}$ has access to all public information on the blockchain. This knowledge enables $\mathbb{A}$ to monitor real-time transactions, account balances, and contract states. This visibility allows for precise timing and execution of attacks.

$\mathbb{AK}_3$ **Economic Dynamics**: $\mathbb{A}$ understands the economic mechanisms governing DEXs and PLFs, including liquidity provision, interest rate calculations, and token valuation. This knowledge is used to manipulate market conditions to the adversary's advantage.

$\mathbb{AK}_4$ **Security Practices**: $\mathbb{A}$ knows security practices, auditing standards, and known vulnerabilities within the DeFi ecosystem. This knowledge can be used to create an effective exploit attack.

$\mathbb{AK}_5$ **Governance Processes**: $\mathbb{A}$ is familiar with the governance models and decision-making processes of target protocols. This includes understanding how proposals are made, voted on, and implemented, allowing the adversary to influence or disrupt governance actions.

$\mathbb{AK}_6$ **Miner Knowledge:** $\mathbb{A}$ has access to pending transactions from private communication channels, and early access to blocks before broadcast if the corresponding miner generates the next block.

$\mathbb{AK}_7$ **Insider knowledge:** $\mathbb{A}$ has access to privileged information such as early access to external market prices, oracle updates, or the wallet passphrases of an operator.

5 VULNERABILITY

Vulnerabilities in Decentralized Finance (DeFi) systems arise from the complex interactions between smart contracts, protocols, and auxiliary services. These vulnerabilities are present across various layers, including the smart contract layer, protocol layer, and network layer, each presenting unique risks to the integrity of DeFi platforms. To classify vulnerabilities of the Critical Infrastructure of Decentralized Finance (DeFi) systems, the vulnerabilities can be categorized based on the system layers where they occur and the types of exploits used by attackers. Vulnerabilities can be broken down into the following categories:

(1) Smart Contract Layer Vulnerabilities ($\mathbb{SCV}$): These vulnerabilities arise from coding errors or flaws in the design of smart contracts. These vulnerabilities include:

Table 1: Mapping of Vulnerabilities to Adversarial Capabilities and Knowledge

Vulnerability	Required Capabilities ($\mathbb{AC}$)	Required Knowledge ($\mathbb{AK}$)
Reentrancy Attack ($\mathbb{SCV}_1$)	$\mathbb{AC}_1, \mathbb{AC}_5$	$\mathbb{AK}_1, \mathbb{AK}_2, \mathbb{AK}_4, \mathbb{AK}_6$
Integer Overflow/Underflow ($\mathbb{SCV}_2$)	$\mathbb{AC}_1, \mathbb{AC}_2$	$\mathbb{AK}_1, \mathbb{AK}_2, \mathbb{AK}_4$
Unchecked External Calls ($\mathbb{SCV}_3$)	$\mathbb{AC}_1$	$\mathbb{AK}_1, \mathbb{AK}_4$
Delegatecall Injection ($\mathbb{SCV}_4$)	$\mathbb{AC}_1, \mathbb{AC}_5$	$\mathbb{AK}_1, \mathbb{AK}_4$
Access Control Issues ($\mathbb{SCV}_5$)	$\mathbb{AC}_1$	$\mathbb{AK}_1, \mathbb{AK}_4$
Oracle Manipulation ($\mathbb{PLV}_1$)	$\mathbb{AC}_3, \mathbb{AC}_5$	$\mathbb{AK}_2, \mathbb{AK}_3, \mathbb{AK}_6, \mathbb{AK}_7$
Flash Loan Exploits ($\mathbb{PLV}_2$)	$\mathbb{AC}_3, \mathbb{AC}_4, \mathbb{AC}_5$	$\mathbb{AK}_2, \mathbb{AK}_3$
Unsafe Dependencies ($\mathbb{PLV}_3$)	$\mathbb{AC}_1, \mathbb{AC}_5$	$\mathbb{AK}_1, \mathbb{AK}_3, \mathbb{AK}_4, \mathbb{AK}_7$
Governance Mechanism ($\mathbb{PLV}_4$)	$\mathbb{AC}_4, \mathbb{AC}_5$	$\mathbb{AK}_3, \mathbb{AK}_5, \mathbb{AK}_7$
Off-Chain Oracle Manipulation ($\mathbb{ASLV}_1$)	$\mathbb{AC}_3, \mathbb{AC}_5$	$\mathbb{AK}_2, \mathbb{AK}_3, \mathbb{AK}_6, \mathbb{AK}_7$
Compromised Private Keys ($\mathbb{ASLV}_2$)	$\mathbb{AC}_3$	$\mathbb{AK}_7$
Phishing Attacks ($\mathbb{ASLV}_3$)	$\mathbb{AC}_5$	$\mathbb{AK}_7$
51% Attack ($\mathbb{CLV}_1$)	$\mathbb{AC}_2, \mathbb{AC}_4$	$\mathbb{AK}_2$
Selfish Mining ($\mathbb{CLV}_2$)	$\mathbb{AC}_2$	$\mathbb{AK}_6$
Transaction Reordering ($\mathbb{CLV}_3$)	$\mathbb{AC}_4, \mathbb{AC}_5$	$\mathbb{AK}_2, \mathbb{AK}_6$

Table 2: Mapping of Attacks to Exploited Vulnerabilities

Attack	Vulnerabilities Exploited
Flash Loan Attacks	Flash Loan Exploits ($\mathbb{PLV}_2$), Oracle Manipulation ($\mathbb{PLV}_2$)
Multi-Vector Attacks	$\mathbb{PLV}_2$, $\mathbb{PLV}_1$, Reentrancy Attack ($\mathbb{SCV}_1$)
Smart Contract Vulnerabilities	$\mathbb{SCV}_1$, $\mathbb{SCV}_2$, $\mathbb{SCV}_3$, $\mathbb{SCV}_5$
Price Manipulation	Oracle Manipulation ($\mathbb{PLV}_1$), Flash Loan Exploits ($\mathbb{PLV}_2$)
Reentrancy Attacks	Reentrancy Attack ($\mathbb{SCV}_1$)
Oracle Manipulation	Oracle Manipulation ($\mathbb{PLV}_1$)
Governance Attacks	Governance Mechanism ($\mathbb{PLV}_4$)
Logic Faults and Bug Exploits	Logic Faults ($\mathbb{SVC}_4$), Unchecked External Calls ($\mathbb{SVC}_3$)
Private Key Compromises	Compromised Private Keys ($\mathbb{ASLV}_2$)
Cross-Chain Bridge Exploits	Cross-Chain Bridge Exploits ($\mathbb{ASLV}_1$)
Sandwich Attacks	Transaction Reordering ($\mathbb{CLV}_3$)
Governance Manipulation	Governance Mechanism ($\mathbb{PLV}_4$)
Rug Pulls	Access Control Issues ($\mathbb{SCV}_5$), Unsafe Dependencies ($\mathbb{PLV}_3$)

$\mathbb{SCV}_1$ Reentrancy Attack: These occur when a smart contract calls an external contract, which then makes recursive calls back to the original function without updating the state, allowing attackers to drain funds.

$\mathbb{SCV}_2$ Integer Overflow/Underflow: These are arithmetic errors that occur when calculations exceed or fall below the allowable range of integers, leading to incorrect behavior of the contract.

$\mathbb{SCV}_3$ Unchecked External Calls: If a contract does not properly verify the outcome of calls to other contracts, it may unknowingly execute malicious functions.

$\mathbb{SCV}_4$ Delegation/Delegatecall Injection: Exploiting the delegatecall function to execute the logic of another contract with the wrong privileges.

$\mathbb{SCV}_5$ Access Control Issues: Improperly implemented permissions or access control can allow unauthorized entities to execute functions meant for administrators only.

(2) Protocol Layer Vulnerabilities ($\mathbb{PLV}$): Vulnerabilities at the protocol design layer often involve market manipulation and unsafe protocol dependencies. These can be classified as follows:

$\mathbb{PLV}_1$ Oracle Manipulation: DeFi protocols often rely on external price oracles for data (e.g., token prices). Manipulating these oracles can result in financial gains, as seen in various price manipulation attacks.

$\mathbb{PLV}_2$ Flash Loan Exploits: Attackers take advantage of flash loans, which are instant uncollateralized loans—to manipulate the market or drain liquidity.

$\mathbb{PLV}_3$ Unsafe Dependencies: Several DeFi protocols interact with external protocols like liquidity pools or yield farming platforms. Flaws in these interactions can lead to exploitation including protocol design flaws. These flaws allows attackers to manipulate the funds.

$\mathbb{PLV}_4$ Governance Mechanism: $\mathbb{A}$ exploits the governance mechanisms by acquiring voting power to manipulate the decision-making process within decentralized autonomous organizations (DAOs).

(3) Auxiliary Service Layer Vulnerabilities ($\mathbb{ASLV}$): These include vulnerabilities related to external services, which can significantly affect the security of DeFi protocols. These services include wallets, off-chain oracles, and web interfaces. These can be classified as follows:

$\mathbb{ASLV}_1$ Off-Chain Oracle Manipulation: Since price data or other information may come from off-chain services, attackers can manipulate these inputs to affect on-chain decisions.

$\mathbb{ASLV}_2$ Compromised Private Keys: Theft or exposure of private keys can give attackers full control over wallets and the assets held within them.

$\mathbb{ASLV}_3$ Phishing Attacks: DeFi users or operators can fall victim to phishing attacks where malicious actors impersonate legitimate services to steal credentials.

(4) Consensus Layer Vulnerabilities ($\mathbb{CLV}$): These are specific to the underlying blockchain consensus mechanisms that maintain the integrity of DeFi platforms. Some common vulnerabilities include:

$\mathbb{CLV}_1$ 51% Attacks: If an attacker gains control of more than 50% of the blockchain's mining or staking power, they can alter the state of the ledger, including rewriting transaction history or double-spending.

$\mathbb{CLV}_2$ Selfish Mining: An attacker strategically withholds blocks they mine to cause disruptions in the blockchain's operation.

$\mathbb{CLV}_3$ Transaction Reordering: Malicious sequencers can manipulate the order of transactions to front-run or back-run other users, extracting additional value from transactions.

Table 1 provides the mapping between vulnerabilities and adversarial capabilities and knowledge that are needed to exploit them. By categorizing vulnerabilities based on the different layers of the DeFi stack, we gain a clearer understanding of the broad attack surface that decentralized systems present. Ensuring robust security requires addressing risks at each layer. This includes the underlying network communication protocols to the interaction of complex financial protocols and auxiliary services.

6 ATTACK ANALYSIS

The analysis of attacks on Decentralized Finance (DeFi) platforms provides critical insights into the methods and strategies employed by adversaries to exploit system vulnerabilities. We analyze 13 major attacks which are listed as follows:

- **Flash Loan Attacks.** Exploits the ability to borrow large amounts of cryptocurrency without collateral to manipulate markets and execute malicious trades within a single transaction.
- **Smart Contract Vulnerabilities.** Exploits flaws in the code of smart contracts, including bugs, reentrancy issues, and improper access control.
- **Price Manipulation.** Involves manipulating the price of assets on DeFi platforms, often through flash loans or oracle manipulations, to profit from artificial price changes.
- **Reentrancy Attacks.** Allows an attacker to repeatedly call a function in a smart contract before the previous function execution is completed, leading to unexpected behaviors and potential fund loss.
- **Oracle Manipulation.** Exploits vulnerabilities in oracles, which are external data providers that feed information into smart contracts, leading to incorrect data being used in transactions.
- **Governance Attacks.** Involves exploiting the governance structures of DeFi platforms, such as voting mechanisms, to pass malicious proposals or gain undue influence.
- **Logic Faults and Bug Exploits.** Targets logical flaws in smart contracts or DeFi protocols, leading to unintended behavior that can be exploited by attackers.
- **Private Key Compromises.** Involves gaining unauthorized access to private keys used in multisig wallets or smart contracts, allowing attackers to control and drain funds.
- **Cross-Chain Bridge Exploits.** Targets vulnerabilities in cross-chain bridges that facilitate transactions between different blockchain networks, leading to the theft of assets during the transfer process.
- **Multi-Vector Attacks.** Combines multiple attack strategies, such as flash loans with oracle manipulation, to maximize the impact of the exploit.
- **Sandwich Attacks.** A form of front-running where an attacker places orders on both sides of a target transaction to profit from the price changes caused by that transaction.
- **Governance Manipulation.** Exploiting governance tokens or systems to influence decisions or actions within a DeFi protocol to the attacker's advantage.
- **Rug Pulls.** When developers or attackers drain funds from a DeFi project and abandon it, often after artificially inflating the value of the tokens.

Table 2 shows the mapping of vulnerabilities that were exploited in each type of attack.

6.1 Data Collection and Analysis

Understanding the nature and frequency of these attacks is essential for developing proactive defenses and reducing the likelihood of future exploits in the DeFi ecosystem. We conduct a novel analysis to further understand and mitigate risks within DEXs and PLFs. We collect the data of incident reports to conduct the risk analysis. This data includes past security incidents and audit reports. This data includes hacks, exploits, and system failures, which we use to analyze patterns and common vulnerabilities. We conduct the following analysis:

- Statistical Analysis: Perform statistical analysis on the collected data to identify trends, correlations, and outliers.
- Risk Scoring: Develop a risk scoring model to quantify the severity and likelihood of potential vulnerabilities. This work involves creating metrics for technical vulnerabilities, economic instability, and governance weaknesses.

The following figures summarize the analysis of the 63 documented incidents from Tables 3, 4, and 5. Figure 1 shows the total losses from 2021 to 2024. Figure 2 shows a heatmap of attack frequency over time. Figure 3 shows the losses due to each attack. Figure 4 shows the frequency of each attack.

The year 2021 marked a significant increase in both the number and severity of attacks on DeFi platforms. A total of $1.8 billion was lost to cybercriminals across 20 documented incidents listed in

Table 3: Summary of Major DeFi Attacks in 2021 (20)

Month	Platform	Amount Lost (USD)	Attack	Platform Type	Notes
2021	Multiple Platforms	$1.8B	Smart Contract Vulnerabilities, Governance Exploits	Mixed (Exchange & Lending)	Significant losses
July	ThorChain	$7.6M	Smart Contract Vulnerability	Exchange	Bifrost protocol exploited
May	PancakeBunny	$200M	Flash Loan Attack	Exchange	Flash loan exploit
August	Cream Finance	$18.8M	Flash Loan Attack	Lending Platform	Large flash loan exploit
December	AscendEX	$77M	Hot Wallet Hack	Exchange	Private key compromise
October	BXH	$139M	Private Key Compromise	Exchange	Key compromise hack
February	Meerkat Finance	$31M	Rug Pull	Mixed (Exchange & Lending)	Sudden platform shutdown
April	Uranium Finance	$50M	Smart Contract Vulnerability	Exchange	Token swap exploit
March	DODO	$3.8M	Smart Contract Vulnerability	Exchange	Flash loan exploit
February	Alpha Finance	$37M	Flash Loan Attack	Lending Platform	Flash loan exploit
November	bZx	$55M	Phishing Attack	Lending Platform	Developer phishing attack
October	Indexed Finance	$16M	Smart Contract Vulnerability	Exchange	Index token manipulation
December	Visor Finance	$8.2M	Reentrancy Attack	Lending Platform	Reentrancy exploit
October	Harvest	$27M	Flash Loan Attack	Exchange	Price differences exploited
January	Harvest Finance	$24M	Flash Loan Attack	Lending Platform	Price oracle manipulation
February	C.R.E.A.M. Finance	$37.5M	Flash Loan Attack	Lending Platform	Flash loan exploit
April	EasyFi	$6M	Private Key Compromise	Lending Platform	Stolen private keys
August	Poly Network	$611M	Cross-Chain Bridge Exploit	Mixed (Exchange & Lending)	Funds later returned by hacker
December	BitMart	$196M	Hot Wallet Hack	Exchange	Private key compromise
August	Liquid Exchange	$97M	Hot Wallet Hack	Exchange	Private key compromise
October	Cream Finance	$130M	Flash Loan Attack	Lending Platform	Flash loan exploit

Tables 3. Notably, the rise of flash loan attacks became a major concern as these attacks exploited the ability to borrow large amounts of cryptocurrency without collateral, manipulate markets, and execute malicious trades within a single transaction. One of the most notable incidents was the Harvest platform attack in October 2021, where a flash loan exploit resulted in the loss of $27 million. This attack highlighted the vulnerability of DeFi platforms to market manipulation, as attackers were able to exploit price differences across different exchanges to drain funds. The total loss due to flash loan attack was over $200 million. Furthermore, numerous platforms experienced a range of vulnerabilities, including reentrancy attacks and flaws within smart contracts. The trend highlights the necessity for enhanced security audits and thorough code evaluations.

Throughout 2022 and 2023, the scale and complexity of attacks on DeFi platforms continue with the trend resulting in a loss of over $2.7 billion across various platforms. Table 4 summarizes 18 major documented incidents of these years. One of the most significant incidents of 2022 occurred on the Maiar Exchange, where a smart contract vulnerability allowed attackers to withdraw approximately $113 million worth of Elrond eGold (EGLD). The most notable incident of 2023 was the Euler Finance hack, where a flash loan attack led to the loss of $197 million, making it the largest DeFi hack of the year. In addition to Euler Finance, Mango Markets suffered a significant attack in January 2023. In this attack, price manipulation was used to exploit the platform which resulted in losses over 117 million USD. This attack highlighted the risks associated with reliance on oracles and the potential for market manipulation in DeFi protocols. The attacks in 2023 revealed the increasing level of sophistication and coordination of the adversaries accross multiple multiple platforms; targeting vulnerabilities in cross-chain protocols.

Throughout 2021 to 2023, attackers increasingly targeted decentralized finance (DeFi) platforms using sophisticated techniques such as bug exploits, logic faults, flash-loan exploits, and private key compromises. The frequency of these attacks highlights a growing trend towards more complex and multi-faceted exploit strategies. The diversity of attacks in 2022 also included oracle manipulations and governance attacks. Adversaries leverage their influence within decentralized autonomous organizations (DAOs) to approve malicious proposals. This demonstrated that on top of technical vulnerabilities; governance structures in DeFi platforms also pose significant risks. In 2023, the emergence of multi-vector attacks was observed; where a single exploit would involve multiple attack methods, such as combining flash loans with oracle manipulation.

The DeFi landscape has significantly matured by 2024, however it continues to face evolving threats summarized in Table 5. The year saw a continuing trend of highly sophisticated attacks, showcasing new strategies as adversaries adapt to the security measures. One of the most significant incidents occurred in July 2024, when an Indian exchange's multisig wallet was hacked in a breach linked to North Korean cybercriminals, resulting in the theft of $235 million. The DeFi ecosystem experienced an increase in sophisticated flash loan attacks. The most notable one being Goledo Finance in January 2024, leading to a $1.7 million loss. Another noteworthy incident

Table 4: Summary of Major DeFi Attacks in 2022-2023 (18)

Date	Platform	Amount Lost (USD)	Attack	Platform Type	Notes
2022	Multiple Platforms	$2.7B	Bug Exploits, Logic Faults, Private Key Compromises	Mixed (Exchange & Lending)	Record losses
June	Maiar Exchange	$113M	Smart Contract Vulnerability	Exchange	Exploit in Elrond blockchain
	Curve Finance	$1.2M	Reentrancy Attack	Exchange	Reentrancy flaw
May	Iron Finance	$2.2M	Price Manipulation	Lending Platform	Stablecoin peg exploited
July	Poly Network	$611M	Cross-Chain Bridge Exploit	Mixed (Exchange & Lending)	Largest DeFi hack in 2022
April	Rari Capital	$80M	Reentrancy Attack	Lending Platform	Fuse pool vulnerability
November	BadgerDAO	$120M	Front-End Exploit	Lending Platform	Phishing attack via front-end
October	Uranium Finance	$50M	Smart Contract Vulnerability	Exchange	Token mispricing exploit
September	Vee Finance	$35M	Smart Contract Vulnerability	Lending Platform	Exploit of Avalanche platform
January	Wormhole	$326M	Cross-Chain Bridge Exploit	Mixed (Exchange & Lending)	Major bridge hack
April	Beanstalk Farms	$182M	Governance Exploit	Lending Platform	Flash loan used for governance takeover
June	Fei Protocol	$10M	Smart Contract Vulnerability	Lending Platform	Exploit in lending platform
September	New Free DAO	$1.25M	Flash Loan Attack	Exchange	Flash loan exploit
August	ZB.com	$4.8M	Hot Wallet Hack	Exchange	Private key compromise
July	Uniswap	$8M	Phishing Attack	Exchange	Fake token phishing
March	Ronin Network	$540M	Private Key Compromise	Mixed (Exchange & Lending)	Largest crypto hack in history
May	Fortress Protocol	$3M	Smart Contract Vulnerability	Lending Platform	Exploit in the BSC network
March 2023	Euler Finance	$197M	Flash Loan Attack	Lending Platform	Largest hack of 2023
January 2023	Mango Markets	$117M	Price Manipulation	Exchange	Oracle manipulation

involved the UwU_Lend platform in June 2024, where an exploit led to the loss of $20 million. This attack once again demonstrated the ongoing risks associated with lending platforms. These attacks often involved manipulating token prices through temporary liquidity provisions which causes a cascading effect across interconnected protocols.

Trend Analysis. Over the years, the nature of DeFi attacks has evolved significantly. The early attacks in 2021 primarily exploited vulnerabilities in smart contracts and governance structures, with flash loan attacks being a predominant threat. As time progressed, the complexity and scale of attacks grew, with 2022 and 2023 witnessing some of the most sophisticated and coordinated exploits, targeting multiple layers of the DeFi ecosystem.

The trend towards more advanced multi-vector attacks in 2023 and 2024 reflects the adaptive strategies employed by cybercriminals as they exploit both technical and governance weaknesses. The increasing integration of DeFi platforms with cross-chain protocols has also introduced new vulnerabilities, making it essential for the industry to adopt more comprehensive security measures.

Overall, the analysis of these incidents highlights the need for continuous improvement in the security practices of DeFi platforms, including regular audits, formal verification of smart contracts, and the implementation of robust governance frameworks to mitigate the risks posed by these increasingly sophisticated threats.

Analysis of major attacks. Based on the attacks summarized in Tables 3, 4, and 5, we draw several insights about the most frequent attacks in the DeFi space.

(1) Smart Contract Vulnerabilities
- Frequency: Smart Contract Vulnerabilities were the most frequently exploited attack.
- Impact: This attack not only occurred most frequently but also resulted in the highest financial losses, totaling an estimated 800 million USD. The prevalence of this attack type suggests that smart contracts are highly susceptible to bugs and vulnerabilities that can be exploited.
- Note: The high frequency of smart contract vulnerabilities indicates the critical importance of rigorous auditing, testing, and formal verification processes in DeFi development. As DeFi platforms increasingly rely on complex smart contracts, ensuring their security becomes critical to protect against these frequent and costly attacks.

(2) Flash Loan Attacks
- Frequency: Flash loan attacks were also highly frequent with 8 documented incidents. This attack involves borrowing large amounts of cryptocurrency without collateral

Table 5: Summary of Major DeFi Attacks in 2024 (17)

Month	Platform	Amount Lost (USD)	Attack	Platform Type	Notes
June	UwU_Lend	$20M	Smart Contract Vulnerability	Lending Platform	Significant loss
July	Unknown Indian Exchange	$235M	Multisig Wallet Hack	Exchange	Linked to North Korea
January	Goledo Finance	$1.7M	Flash Loan Attack	Lending Platform	Token price manipulation
May	VeloCore	$6.88M	Lack of Access Control	Exchange	Multi-chain exploit
May	NORMIE	$490K	Business Logic Flow	Exchange	Logic flaw exploited
June	MineSTM	13.6K SOL	Business Logic Flow	Exchange	Business logic flaw
May	SCROLL	293K (76 ETH)	Integer Underflow	Exchange	Bug exploited
May	Sonne Finance	$20M	Precision Loss	Lending Platform	Contract flaw
April	HedgeyFinance	$48M	Logic Flow	Lending Platform	Logic exploit
April	PikeFinance	$1.4M (479 ETH)	Uninitialized Proxy	Lending Platform	Proxy contract issue
April	Rico	36K ETH	Arbitrary Call	Lending Platform	Arbitrary call exploit
April	UPS	28K ETH	Business Logic Flaw	Exchange	Logic flaw exploited
April	SQUID	87K BSC (ETH)	Sandwich Attack	Exchange	Transaction order manipulation
April	OpenLeverage	234K BSC (ETH)	Reentrancy Attack	Lending Platform	Reentrancy exploit
May	PredyFinance	464K Arbitrum (ETH)	Reentrancy Attack	Lending Platform	Reentrancy flaw
May	TSURU	140K ETH	Insufficient Validation	Exchange	Validation issue exploited
May	SATURN	600 BSC (ETH)	Price Manipulation	Exchange	Oracle manipulation

to manipulate price oracles or exploit vulnerabilities in smart contracts.

- Impact: Flash loan attacks have caused substantial financial losses, with an estimated 300 million USD lost across various incidents.
- Note: Flash loan attacks highlight the risks associated with the instant liquidity provided by DeFi platforms. These attacks are often combined with other exploit techniques to amplify their impact. The frequency and success of these attacks suggest that DeFi platforms need to implement more robust mechanisms to detect and prevent flash loan exploits.

(3) Multi-Vector Attacks
- Frequency: Multi-vector attacks, which combine multiple attack strategies are quite common with 7 major recored incidents. These attacks are particularly difficult to prevent as they exploit several vulnerabilities simultaneously.
- Impact: Multi-vector attacks resulted in losses over $450 million.
- Note: The increasing frequency of multi-vector attacks indicates a trend toward more sophisticated and coordinated exploit strategies. As attackers become more adept at combining different attacks, DeFi platforms must adopt comprehensive security measures that address multiple types of vulnerabilities simultaneously.

(4) Price Manipulation
- Frequency: Price manipulation attacks were moderately frequent, with 6 incidents documented. These attacks often involve manipulating the price of assets on DeFi platforms, usually through flash loans or oracle manipulations.
- Impact: This attack led to over $150 million in financial losses.
- Note: Price manipulation remains a significant threat to DeFi platforms, especially those relying on oracles for price feeds. The moderate frequency but substantial impact of these attacks underscores the need for more reliable and secure oracle solutions in DeFi protocols.

(5) Cross-chain bridge exploits:
- Frequency: Cross-chain bridge exploits were less frequent than other attacks with only 3 documented incidents. However, despite their lower frequency, these attacks are notable for their potential to cause massive financial losses.
- Impact: Cross-chain bridge exploits have resulted in substantial financial losses over $700 million USD.
- Note: Cross-chain bridge exploits target the infrastructure that facilitates transactions between different blockchain networks. These bridges are critical for enabling interoperability in the DeFi ecosystem, but their complexity and the large sums of assets they manage make them attractive targets for attackers. The Poly Network hack in July 2022, which resulted in a loss of $611 million, stands out as one of the largest single loss incidents in DeFi history. This event underscores the critical need for stronger security protocols in cross-chain technologies.

The attack that caused the highest financial loss was the exploitation of Smart Contract Vulnerabilities, with a hypothetical total loss of 800 million USD. This suggests that issues in smart contract

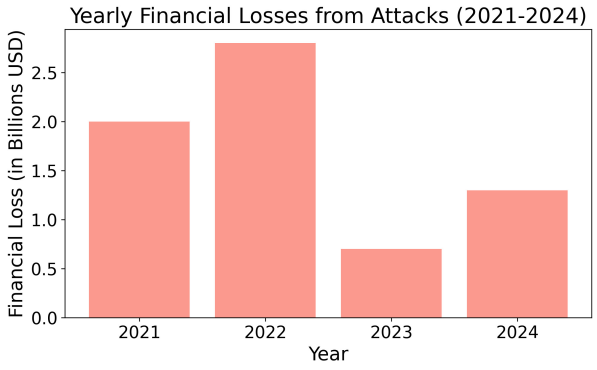

Figure 1: Total Losses from 2021 to 2024

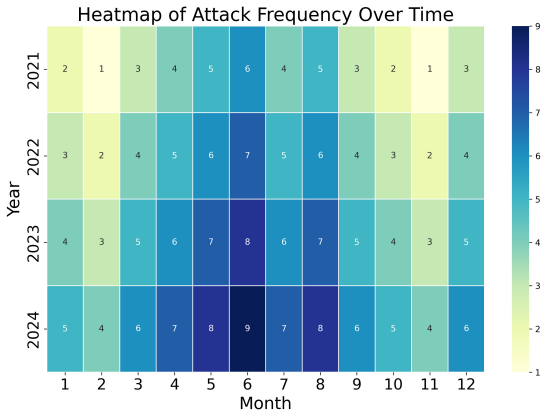

Figure 2: Heatmap of Attack Frequency over Time

code are a significant risk in the DeFi space. These findings suggest that while DeFi continues to innovate, the security landscape must evolve to address these persistent and emerging threats. By understanding the most frequent and damaging attacks, DeFi operators can better prioritize security measures to mitigate the risks posed by these common exploit strategies.

7 DEFENSE

The defense strategies involve assessing the potential impact of various risks and prioritizing mitigation efforts. We use the Risk Matrix and Failure Modes and Effects Analysis (FMEA) approach. To combine the Risk Matrix and FMEA (Failure Modes and Effects Analysis) approaches, we develop a risk analysis model that assesses these risks based on their likelihood, impact, and additional factors such as detectability. This hybrid approach provides a thorough evaluation of risks, allowing for both qualitative and quantitative assessments. The following is the approach of the analysis:

(1) Risk Identification: First, identify all potential risks associated with the DeFi platform. These could include technical risks (e.g., smart contract vulnerabilities), operational risks (e.g., governance failures), and external risks (e.g., regulatory changes).
(2) Risk Categorization using Risk Matrix:
   - Likelihood: Rate the likelihood of each risk occurring on a scale (e.g., 1 to 5, where 1 = very unlikely and 5 = very likely).
   - Impact: Evaluate the potential impact of each risk if it occurs, also on a scale (e.g., 1 to 5, where 1 = minor and 5 = critical).
   - Risk Matrix Placement: Place each risk into a Risk Matrix based on its likelihood and impact. This will help in visualizing the relative importance of each risk.
   - Table 6 shows the risk matrix.
(3) FMEA Analysis for Each Risk:
   - Impact: Use the impact rating from the Risk Matrix (1 to 5).
   - Likelihood: Use the likelihood rating from the Risk Matrix (1 to 5).
   - Detectability: Assign a detectability score (1 to 5), where 1 means the risk is easily detectable, and 5 means it's hard to detect.
   - Calculate the Risk Priority Number (*RPN*): Multiply the scores for severity (S), likelihood (L), and detectability (D) to calculate the RPN:

$$RPN = S \cdot L \cdot D$$

   - Prioritize Risks: Rank the risks based on their RPN values. Higher RPN values indicate higher priority risks that require immediate attention.
(4) Mitigation Strategies Based on RPN:
   - High RPN Risks (Critical Risks): Immediate action is required. Implement preventive controls and improve detection methods.
   - Moderate RPN Risks (High Risks): Develop and apply mitigation strategies to reduce likelihood, impact, or improve detectability.
   - Low RPN Risks (Moderate to Low Risks): Monitor these risks but prioritize resources towards higher RPN risks.
(5) Periodic Review and Update: Regularly review the risk matrix and FMEA results as new risks emerge in the DeFi space. Adjust the RPN calculations and mitigation strategies as necessary.

This combined approach of using risk matrix and FMEA allows to:

- Identify and categorize risks quickly using a risk matrix.
- Quantify the priority of each risk through FMEA, incorporating detectability as a crucial factor.
- Prioritize resources and actions based on the RPN, ensuring that the most critical risks are addressed first.

7.1 FMEA Table

To create an FMEA table with all 13 attacks based on the statistical analysis of the 63 incidents from the three tables, we assess the Severity (S), Likelihood (L), and Detectability (D) for each attack. These are calculated from the historical data. The explanation of how each component can be derived is as follows:

- Severity (S): It is based on the financial losses associated with each attack. Table 7 shows the criteria used to determine the severity level.

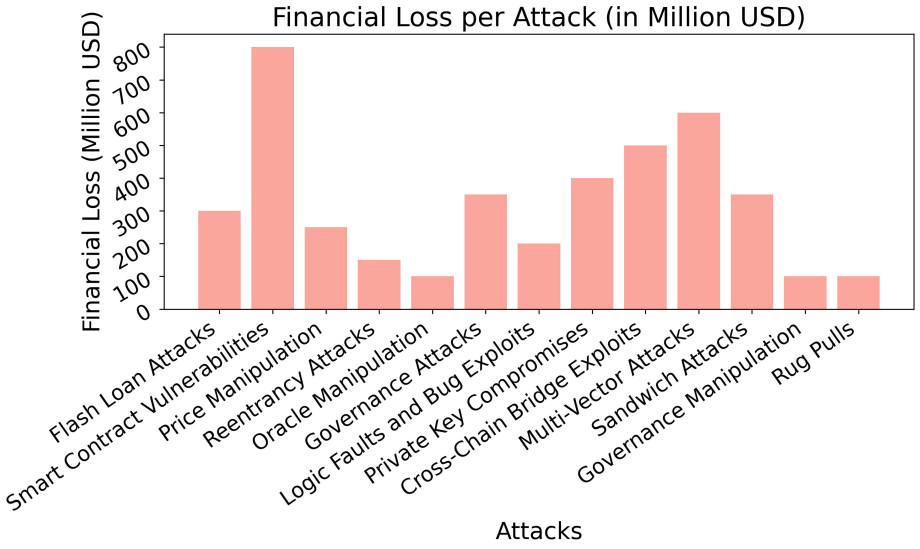

Figure 3: Financial loss (in Million USD) per attack

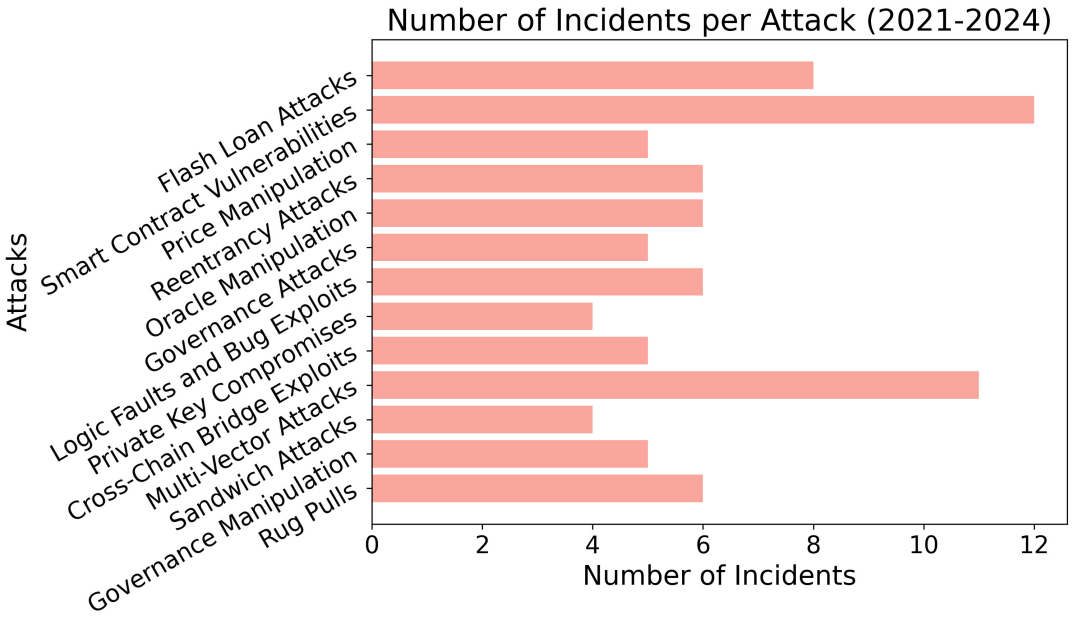

Figure 4: Frequency of 13 attacks

Table 6: Risk matrix categorizing risks based on likelihood and impact

Likelihood \Impact	Low Impact (1)	Medium Impact (2-3)	High Impact (4-5)
Low (1-2)	Low Risk	Low-Moderate Risk	Moderate Risk
Medium (3)	Low-Moderate Risk	Moderate Risk	High Risk
High (4-5)	Moderate Risk	High Risk	Critical Risk

Table 7: Risk severity based on financial impact

Severity Level	Monetary Loss
Low (1)	$< \$10M$
Moderate (2)	$\$10M - \$25M$
Significant (3)	$\$25M - \$50M$
High (4)	$\$50M - \$100M$
Critical (5)	$> \$100M$

Table 8: Risk likelyhood based on frequency of incidents

Likelyhood Level	Frequency
Low (1)	$0 - 1$
Moderate (2)	$2 - 3$
Significant (3)	$4 - 5$
High (4)	$5 - 6$
Critical (5)	> 7

- Likelihood (L): It is derived from the frequency of incidents for each attack (based on the pie chart of incidents). Table 8 shows the criteria used to determine the likelyhood of incidents.
- Detectability (D): This metric represents how easy it is to detect the risk before it materializes. Attacks that are harder to detect, such as smart contract vulnerabilities or cross-chain exploits, would score higher on this metric, whereas more visible attacks, like flash loan attacks, would score lower.

To assign detectability scores objectively, we use empirical data, measurable factors, and quantitative assessment. Here is the list of factors we use to determine the detectibility score.

(1) Audit Frequency: This reflects how often audits or code reviews are conducted for each type of vulnerability. More frequent audits typically result in higher detectability. For example, smart contract vulnerabilities might be easier to detect on platforms that regularly undergo formal verification or third-party audits.
(2) Availability of Detection Tools: Use objective measures of available detection tools for each attack. Some attacks, like flash loans, have specialized detection tools that allow platforms to monitor suspicious transactions in real-time. Other vectors, such as private key compromises lack such tools which makes them harder to detect.
(3) Historical Success of Attack Detection: This metric is based on historical data from past attacks. If several incidents of a particular attack have been detected or prevented before exploitation, it suggests a higher detectability.
(4) Time to Detect: Use the average time it takes to detect each type of attack (post-incident reports, audits). It is measured by the amount of time it typically takes platforms to detect the attack post-incident. A longer detection window suggests lower detectability.

Table 9 provides detectability scores for the 13 attacks based on the four aforementioned factors. Table 10 provides an FMEA table for the 13 attacks based on the statistical analysis of the data. Below are the recommendations based on calculated RPN:

- RPN greater than 75. Smart Contract Vulnerabilities (RPN: 75) should be prioritized for mitigation, as they have the highest risk. This risk comes with high severity, high likelihood, and moderate detectability.
- RPN ranging from 20 to 75. Cross-Chain Bridge Exploits (RPN: 50) and Flash Loan Attacks (RPN: 48) also require focused mitigation efforts due to their critical financial impact and frequency.
- RPN lower than 20. Low-Risk Vectors such as Sandwich Attacks (RPN: 8) and Rug Pulls (RPN: 12) can be monitored, but they pose less of a risk compared to higher RPN vectors.

Using this approach makes it easier to identify, assess, and mitigate potential threats effectively. This approach not only helps in current risk management but also sets the foundation for continuous monitoring and improvement as the ecosystem evolves.

8 DISCUSSION

Despite significant advancements in the DeFi ecosystem, several critical gaps remain in both research and practice that must be addressed to ensure the continued security and stability of DeFi platforms. There has been substantial work on identifying vulnerabilities in smart contracts and DeFi protocols; however, there is limited research on how to systematically mitigate these vulnerabilities beyond basic auditing and formal verification techniques. Several DeFi platforms still rely on reactive rather than proactive defenses, responding to attacks after they occur rather than employing preventive measures designed to anticipate potential exploits.

Current threat models tend to focus on individual attack vectors but often fail to consider multi-vector attacks where adversaries combine different techniques to exploit multiple layers simultaneously. Future research could focus on developing more dynamic and adaptive threat models that can account for this increasing complexity. This research may include cross-chain interactions and new financial instruments to expand the DeFi landscape.

Table 9: Detectability Score Table for DeFi Attacks Based on Objective Criteria

Attack	Audit Frequency	Availability of Tools	Historical Success	Time to Detect	D Score
Flash Loan Attacks	Frequent	Widely available	Mixed success	Quick	2
Smart Contract Vulnerabilities	Common	Auditing tools	Mixed success	Late	3
Price Manipulation	Moderate	Tools for oracles	Moderate success	Early	2
Reentrancy Attacks	Infrequent	Few tools	Rare detection	Late	4
Oracle Manipulation	Moderate	Tools for oracles	Moderate success	Early	3
Governance Attacks	Rare	Limited tools	Rare detection	Late	5
Logic Faults and Bug Exploits	Moderate	Limited tools	Moderate success	Late	3
Private Key Compromises	Infrequent	No tools	Rare detection	Late	5
Cross-Chain Bridge Exploits	Rare	Few tools	Rare detection	Late	5
Multi-Vector Attacks	Moderate	Some tools	Mixed success	Quick	3
Sandwich Attacks	Frequent	Widely available	High success rate	early	2
Governance Manipulation	Rare	Few tools	Rare detection	Late	4
Rug Pulls	Moderate	No tools	Rare detection	Quick	3

Table 10: FMEA Table for DeFi Attacks with Risk Priority Numbers (RPN)

Attack	Severity (S)	Likelihood (L)	Detectability (D)	RPN (S × L × D)
Flash Loan Attacks	4	4	2	32
Smart Contract Vulnerabilities	5	5	3	75
Price Manipulation	3	3	2	18
Reentrancy Attacks	3	2	4	24
Oracle Manipulation	4	3	3	36
Governance Attacks	3	2	5	30
Logic Faults and Bug Exploits	3	3	3	27
Private Key Compromises	5	1	5	25
Cross-Chain Bridge Exploits	5	2	5	50
Multi-Vector Attacks	4	4	3	48
Sandwich Attacks	2	2	2	8
Governance Manipulation	3	3	4	36
Rug Pulls	2	3	3	18

9 CONCLUSION

This paper presents a comprehensive risk analysis survey for the critical infrastructure of DeFi, focusing on DEXs and PLFs. By examining the protocol design and smart contract layers, we identify key vulnerabilities and propose mitigation strategies from technical, economic, and governance perspectives. We propose a novel risk scoring model to quantify the severity and likelihood of risk based on technical, economical, and governance factors. The proposed guidelines and case studies aim to enhance the security and resilience of DeFi platforms, contributing to a more stable decentralized financial ecosystem. For future research, we should continue to explore emerging risks and develop adaptive strategies to keep pace with the rapid evolution of DeFi.

REFERENCES

[1] 2021. Defiranger: Detecting price manipulation attacks on defi applications. *arXiv preprint arXiv:2104.15068* (2021).

[2] Hendrik Amler, Lisa Eckey, Sebastian Faust, Marcel Kaiser, Philipp Sandner, and Benjamin Schlosser. 2021. Defi-ning defi: Challenges & pathway. In *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 181–184.

[3] Kushal Babel, Mojan Javaheripi, Yan Ji, Mahimna Kelkar, Farinaz Koushanfar, and Ari Juels. 2023. Lanturn: Measuring Economic Security of Smart Contracts Through Adaptive Learning. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (<conf-loc>, <city>Copenhagen</city>, <country>Denmark</country>, </conf-loc>) *(CCS '23)*. Association for Computing Machinery, New York, NY, USA, 1212–1226. https://doi.org/10.1145/3576915.3623204

[4] Carsten Baum, James Hsin-yu Chiang, Bernardo David, Tore Kasper Frederiksen, and Lorenzo Gentile. 2022. Sok: Mitigation of front-running in decentralized finance. In *International Conference on Financial Cryptography and Data Security*. Springer, 250–271.

[5] Felix Bekemeier. 2022. Deceptive Assurance? A Conceptual View on Systemic Risk in Decentralized Finance (DeFi). In *Proceedings of the 2021 4th International Conference on Blockchain Technology and Applications* (Xi'an, China) *(ICBTA '21)*. Association for Computing Machinery, New York, NY, USA, 76–87. https://doi.org/10.1145/3510487.3510499

[6] Lexi Brent, Neville Grech, Sifis Lagouvardos, Bernhard Scholz, and Yannis Smaragdakis. 2020. Ethainter: a smart contract security analyzer for composite vulnerabilities. In *Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation* (London, UK) *(PLDI 2020)*. Association for Computing Machinery, New York, NY, USA, 454–469. https://doi.org/10.1145/3385412.3385990

[7] Yixin Cao, Chuanwei Zou, and Xianfeng Cheng. 2021. Flashot: a snapshot of flash loan attack on DeFi ecosystem. *arXiv preprint arXiv:2102.00626* (2021).

[8] Nic Carter and Linda Jeng. 2021. DeFi protocol risks: The paradox of DeFi. *Regtech, suptech and beyond: innovation and technology in financial services" riskbooks–forthcoming Q* 3 (2021).

[9] Federico Cernera, Massimo La Morgia, Alessandro Mei, Alberto Maria Mongardini, and Francesco Sassi. 2023. Ready, Aim, Snipe! Analysis of Sniper Bots and their Impact on the DeFi Ecosystem. In *Companion Proceedings of the ACM Web*

Conference 2023 (<conf-loc>, <city>Austin</city>, <state>TX</state>, <country>USA</country>, </conf-loc>) *(WWW '23 Companion)*. Association for Computing Machinery, New York, NY, USA, 1093–1102. https://doi.org/10.1145/3543873.3587612

[10] Stefanos Chaliasos, Marcos Antonios Charalambous, Liyi Zhou, Rafaila Galanopoulou, Arthur Gervais, Dimitris Mitropoulos, and Ben Livshits. 2023. Smart contract and defi security: Insights from tool evaluations and practitioner surveys. *arXiv preprint arXiv:2304.02981* (2023).

[11] Ting Chen, Rong Cao, Ting Li, Xiapu Luo, Guofei Gu, Yufei Zhang, Zhou Liao, Hang Zhu, Gang Chen, Zheyuan He, et al. 2020. SODA: A Generic Online Detection Framework for Smart Contracts.. In *NDSS*.

[12] Ting Chen, Xiaoqi Li, Ying Wang, Jiachi Chen, Zihao Li, Xiapu Luo, Man Ho Au, and Xiaosong Zhang. 2017. An Adaptive Gas Cost Mechanism for Ethereum to Defend Against Under-Priced DoS Attacks. https://doi.org/10.1007/978-3-319-72359-4_1

[13] Zhiyang Chen, Sidi Mohamed Beillahi, and Fan Long. 2024. Flashsyn: Flash loan attack synthesis via counter example driven approximation. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*. 1–13.

[14] Tarun Chitra and Kshitij Kulkarni. 2022. Improving Proof of Stake Economic Security via MEV Redistribution. In *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security* (Los Angeles, CA, USA) *(DeFi'22)*. Association for Computing Machinery, New York, NY, USA, 1–7. https://doi.org/10.1145/3560832.3564259

[15] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2020. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE symposium on security and privacy (SP)*. IEEE, 910–927.

[16] Dipanjan Das, Priyanka Bose, Nicola Ruaro, Christopher Kruegel, and Giovanni Vigna. 2022. Understanding Security Issues in the NFT Ecosystem. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (Los Angeles, CA, USA) *(CCS '22)*. Association for Computing Machinery, New York, NY, USA, 667–681. https://doi.org/10.1145/3548606.3559342

[17] Xun Deng, Sidi Mohamed Beillahi, Cyrus Minwalla, Han Du, Andreas Veneris, and Fan Long. 2024. Safeguarding DeFi Smart Contracts against Oracle Deviations. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*. 1–12.

[18] Yepeng Ding, Arthur Gervais, Roger Wattenhofer, and Hiroyuki Sato. 2024. Hunting DeFi Vulnerabilities via Context-Sensitive Concolic Verification. *arXiv preprint arXiv:2404.10376* (2024).

[19] Li Duan, Yangyang Sun, Kejia Zhang, Yong Ding, and Yuling Chen. 2022. Multiple-Layer Security Threats on the Ethereum Blockchain and Their Countermeasures. *Sec. and Commun. Netw.* 2022 (jan 2022), 11 pages. https://doi.org/10.1155/2022/5307697

[20] Rundong Gan, Le Wang, and Xiaodong Lin. 2023. Why Trick Me: The Honeypot Traps on Decentralized Exchanges. In *Proceedings of the 2023 Workshop on Decentralized Finance and Security* (<conf-loc>, <city>Copenhagen</city>, <country>Denmark</country>, </conf-loc>) *(DeFi '23)*. Association for Computing Machinery, New York, NY, USA, 17–23. https://doi.org/10.1145/3605768.3623546

[21] Rundong Gan, Le Wang, Xiangyu Ruan, and Xiaodong Lin. 2023. Understanding Flash-Loan-based Wash Trading. In *Proceedings of the 4th ACM Conference on Advances in Financial Technologies* (Cambridge, MA, USA) *(AFT '22)*. Association for Computing Machinery, New York, NY, USA, 74–88. https://doi.org/10.1145/3558535.3559793

[22] Krzysztof Gogol, Christian Killer, Malte Schlosser, Thomas Bocek, Burkhard Stiller, and Claudio Tessone. 2024. SoK: Decentralized Finance (DeFi)–Fundamentals, Taxonomy and Risks. *arXiv preprint arXiv:2404.11281* (2024).

[23] Lewis Gudgeon, Sam Werner, Daniel Perez, and William J. Knottenbelt. 2020. DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies* (New York, NY, USA) *(AFT '20)*. Association for Computing Machinery, New York, NY, USA, 92–112. https://doi.org/10.1145/3419614.3423254

[24] Campbell R Harvey, Ashwin Ramachandran, and Joey Santoro. 2021. *DeFi and the Future of Finance*. John Wiley & Sons.

[25] Lioba Heimbach and Roger Wattenhofer. 2022. Eliminating Sandwich Attacks with the Help of Game Theory. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security* (Nagasaki, Japan) *(ASIA CCS '22)*. Association for Computing Machinery, New York, NY, USA, 153–167. https://doi.org/10.1145/3488932.3517390

[26] Nikolay Ivanov, Chenning Li, Qiben Yan, Zhiyuan Sun, Zhichao Cao, and Xiapu Luo. 2023. Security Threat Mitigation for Smart Contracts: A Comprehensive Survey. *ACM Comput. Surv.* 55, 14s, Article 326 (jul 2023), 37 pages. https://doi.org/10.1145/3593293

[27] G. Karame and S. Capkun. 2018. Blockchain Security and Privacy. *IEEE Security & Privacy* 16, 04 (jul 2018), 11–12. https://doi.org/10.1109/MSP.2018.3111241

[28] Gurdip Kaur, Arash Habibi Lashkari, Iman Sharafaldin, and Ziba Habibi Lashkari. 2023. Smart contracts and defi security and threats. In *Understanding Cybersecurity Management in Decentralized Finance: Challenges, Strategies, and Trends*. Springer, 91–111.

[29] Stefan Kitzler, Friedhelm Victor, Pietro Saggese, and Bernhard Haslhofer. 2023. Disentangling Decentralized Finance (DeFi) Compositions. *ACM Trans. Web* 17, 2, Article 10 (mar 2023), 26 pages. https://doi.org/10.1145/3532857

[30] Ariah Klages-Mundt, Dominik Harz, Lewis Gudgeon, Jun-You Liu, and Andreea Minca. 2020. Stablecoins 2.0: Economic Foundations and Risk-based Models. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies* (New York, NY, USA) *(AFT '20)*. Association for Computing Machinery, New York, NY, USA, 59–79. https://doi.org/10.1145/3419614.3423261

[31] Queping Kong, Jiachi Chen, Yanlin Wang, Zigui Jiang, and Zibin Zheng. 2023. DeFiTainter: Detecting Price Manipulation Vulnerabilities in DeFi Protocols. In *Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis* (<conf-loc>, <city>Seattle</city>, <state>WA</state>, <country>USA</country>, </conf-loc>) *(ISSTA 2023)*. Association for Computing Machinery, New York, NY, USA, 1144–1156. https://doi.org/10.1145/3597926.3598124

[32] Wenkai Li, Jiuyang Bu, Xiaoqi Li, and Xianyi Chen. 2022. Security analysis of DeFi: Vulnerabilities, attacks and advances. In *2022 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 488–493.

[33] Wenkai Li, Jiuyang Bu, Xiaoqi Li, Hongli Peng, Yuanzheng Niu, and Yuqing Zhang. 2022. A survey of DeFi security: Challenges and opportunities. *Journal of King Saud University-Computer and Information Sciences* 34, 10 (2022), 10378–10404.

[34] Weilin Li, Zhun Wang, Chenyu Li, Heying Chen, Taiyu Wong, Pengyu Sun, Yufei Yu, and Chao Zhang. 2023. Unmasking Role-Play Attack Strategies in Exploiting Decentralized Finance (DeFi) Systems. In *Proceedings of the 2023 Workshop on Decentralized Finance and Security* (<conf-loc>, <city>Copenhagen</city>, <country>Denmark</country>, </conf-loc>) *(DeFi '23)*. Association for Computing Machinery, New York, NY, USA, 33–39. https://doi.org/10.1145/3605768.3623545

[35] Xiaofan Li, Jin Yang, Jiaqi Chen, Yuzhe Tang, and Xing Gao. 2024. Characterizing Ethereum Upgradable Smart Contracts and Their Security Implications. In *Proceedings of the ACM on Web Conference 2024* (<conf-loc>, <city>Singapore</city>, <country>Singapore</country>, </conf-loc>) *(WWW '24)*. Association for Computing Machinery, New York, NY, USA, 1847–1858. https://doi.org/10.1145/3589334.3645640

[36] Zihao Li, Jianfeng Li, Zheyuan He, Xiapu Luo, Ting Wang, Xiaoze Ni, Wenwu Yang, Xi Chen, and Ting Chen. 2023. Demystifying DeFi MEV Activities in Flashbots Bundle. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (<conf-loc>, <city>Copenhagen</city>, <country>Denmark</country>, </conf-loc>) *(CCS '23)*. Association for Computing Machinery, New York, NY, USA, 165–179. https://doi.org/10.1145/3576915.3616590

[37] Z. Li, B. Xiao, S. Guo, and Y. Yang. 2023. Securing Deployed Smart Contracts and DeFi With Distributed TEE Cluster. *IEEE Transactions on Parallel and Distributed Systems* 34, 03 (mar 2023), 828–842. https://doi.org/10.1109/TPDS.2022.3232548

[38] Qiushan Liu, Lang Yu, and Chang Jia. 2020. MovER: Stabilize Decentralized Finance System with Practical Risk Management. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. 55–56. https://doi.org/10.1109/BRAINS49436.2020.9223274

[39] Yulin Liu, Yuxuan Lu, Kartik Nayak, Fan Zhang, Luyao Zhang, and Yinhong Zhao. 2022. Empirical Analysis of EIP-1559: Transaction Fees, Waiting Times, and Consensus Security. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (Los Angeles, CA, USA) *(CCS '22)*. Association for Computing Machinery, New York, NY, USA, 2099–2113. https://doi.org/10.1145/3548606.3559341

[40] Loi Luu, Jason Teutsch, Raghav Kulkarni, and Prateek Saxena. 2015. Demystifying Incentives in the Consensus Computer. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (Denver, Colorado, USA) *(CCS '15)*. Association for Computing Machinery, New York, NY, USA, 706–719. https://doi.org/10.1145/2810103.2813659

[41] Conor McMenamin, Vanesa Daza, Matthias Fitzi, and Padraic O'Donoghue. 2022. FairTraDEX: A Decentralised Exchange Preventing Value Extraction. In *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security* (Los Angeles, CA, USA) *(DeFi'22)*. Association for Computing Machinery, New York, NY, USA, 39–46. https://doi.org/10.1145/3560832.3563439

[42] Jason Milionis, Ciamac C. Moallemi, Tim Roughgarden, and Anthony Lee Zhang. 2022. Quantifying Loss in Automated Market Makers. In *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security* (Los Angeles, CA, USA) *(DeFi'22)*. Association for Computing Machinery, New York, NY, USA, 71–74. https://doi.org/10.1145/3560832.3563441

[43] Benedikt Putz, Manfred Vielberth, and Günther Pernul. 2022. BISCUIT - Blockchain Security Incident Reporting based on Human Observations. In *Proceedings of the 17th International Conference on Availability, Reliability and Security* (Vienna, Austria) *(ARES '22)*. Association for Computing Machinery, New York, NY, USA, Article 27, 6 pages. https://doi.org/10.1145/3538969.3538984

[44] Kaihua Qin and Fan Zhang. 2023. DeFi '23: Workshop on Decentralized Finance and Security. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (<conf-loc>, <city>Copenhagen</city>, <country>Denmark</country>, </conf-loc>) *(CCS '23)*. Association for Computing Machinery, New York, NY, USA, 3660–3661. https://doi.org/10.1145/3576915.3624026

[45] Kaihua Qin, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. 2021. An empirical study of DeFi liquidations: incentives, risks, and instabilities. In *Proceedings of the 21st ACM Internet Measurement Conference* (Virtual Event) *(IMC '21)*. Association for Computing Machinery, New York, NY, USA, 336–350. https://doi.org/10.1145/3487552.3487811

[46] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. 2021. Attacking the defi ecosystem with flash loans for fun and profit. In *International conference on financial cryptography and data security*. Springer, 3–32.

[47] S. Dos Santos, J. Singh, R. K. Thulasiram, S. Kamali, L. Sirico, and L. Loud. 2022. A New Era of Blockchain-Powered Decentralized Finance (DeFi) - A Review. In *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE Computer Society, Los Alamitos, CA, USA, 1286–1292. https://doi.org/10.1109/COMPSAC54236.2022.00203

[48] J. Su, X. Lin, Z. Fang, Z. Zhu, J. Chen, Z. Zheng, W. Lv, and J. Wang. 2023. DeFiWarder: Protecting DeFi Apps from Token Leaking Vulnerabilities. In *2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE)*. IEEE Computer Society, Los Alamitos, CA, USA, 1664–1675. https://doi.org/10.1109/ASE56229.2023.00110

[49] Xinyuan Sun, Shaokai Lin, Vilhelm Sjöberg, and Jay Jie. 2021. How to Exploit a DeFi Project. In *Financial Cryptography and Data Security. FC 2021 International Workshops: CoDecFin, DeFi, VOTING, and WTSC, Virtual Event, March 5, 2021, Revised Selected Papers 25*. Springer, 162–167.

[50] Bin Wang, Han Liu, Chao Liu, Zhiqiang Yang, Qian Ren, Huixuan Zheng, and Hong Lei. 2021. Blockeye: Hunting for defi attacks on blockchain. In *2021 IEEE/ACM 43rd international conference on software engineering: companion proceedings (ICSE-companion)*. IEEE, 17–20.

[51] Bin Wang, Xiaohan Yuan, Li Duan, Hongliang Ma, Chunhua Su, and Wei Wang. 2022. DeFiScanner: Spotting DeFi attacks exploiting logic vulnerabilities on blockchain. *IEEE Transactions on Computational Social Systems* (2022).

[52] Chenmin Wang, Peng Li, Yulong Zeng, and Xuepeng Fan. 2024. Optimal Flash Loan Fee Function with Respect to Leverage Strategies. In *Proceedings of the 23rd International Conference on Autonomous Agents and Multiagent Systems* (<conf-loc>, <city>Auckland</city>, <country>New Zealand</country>, </conf-loc>) *(AAMAS '24)*. International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 1874–1882.

[53] Qin Wang, Rujia Li, Qi Wang, Shiping Chen, and Yang Xiang. 2022. Exploring Unfairness on Proof of Authority: Order Manipulation Attacks and Remedies. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security* (Nagasaki, Japan) *(ASIA CCS '22)*. Association for Computing Machinery, New York, NY, USA, 123–137. https://doi.org/10.1145/3488932.3517394

[54] S. Wang, C. Wu, Y. Liang, L. Hsieh, and H. Hsiao. 2021. ProMutator: Detecting Vulnerable Price Oracles in DeFi by Mutated Transactions. In *2021 IEEE European Symposium on Security and Privacy Workshops*. IEEE Computer Society, Los Alamitos, CA, USA, 380–385. https://doi.org/10.1109/EuroSPW54576.2021.00047

[55] Ye Wang, Patrick Zuest, Yaxing Yao, Zhicong Lu, and Roger Wattenhofer. 2022. Impact and user perception of sandwich attacks in the defi ecosystem. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–15.

[56] Zhipeng Wang, Kaihua Qin, Duc Vu Minh, and Arthur Gervais. 2022. Speculative Multipliers on DeFi: Quantifying On-Chain Leverage Risks. In *Financial Cryptography and Data Security*, Ittay Eyal and Juan Garay (Eds.). Springer International Publishing, Cham, 38–56.

[57] Sam Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William Knottenbelt. 2022. Sok: Decentralized finance (defi). In *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*. 30–46.

[58] Matheus Venturyne Xavier Ferreira and David C Parkes. 2023. Credible decentralized exchange design via verifiable sequencing rules. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 723–736.

[59] Jiahua Xu, Krzysztof Paruch, Simon Cousaert, and Yebo Feng. 2023. SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols. *ACM Comput. Surv.* 55, 11, Article 238 (feb 2023), 50 pages. https://doi.org/10.1145/3570639

[60] Teng Andrea Xu and Jiahua Xu. 2022. A short survey on business models of decentralized finance (DeFi) protocols. In *International Conference on Financial Cryptography and Data Security*. Springer, 197–206.

[61] Kailun Yan, Jilian Zhang, Xiangyu Liu, Wenrui Diao, and Shanqing Guo. 2023. Bad Apples: Understanding the Centralized Security Risks in Decentralized Ecosystems. In *Proceedings of the ACM Web Conference 2023* (<conf-loc>, <city>Austin</city>, <state>TX</state>, <country>USA</country>, </conf-loc>) *(WWW '23)*. Association for Computing Machinery, New York, NY, USA, 2274–2283. https://doi.org/10.1145/3543507.3583393

[62] Yinjie Zhao, Xin Kang, Tieyan Li, Cheng-Kang Chu, and Haiguang Wang. 2022. Toward trustworthy defi oracles: past, present, and future. *IEEE Access* 10 (2022), 60914–60928.

[63] Liyi Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits, and Arthur Gervais. 2021. On the just-in-time discovery of profit-generating transactions in defi protocols. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 919–936.

[64] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc V Le, and Arthur Gervais. 2021. High-frequency trading on decentralized on-chain exchanges. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 428–445.

[65] Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. 2023. Sok: Decentralized finance (defi) attacks. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2444–2461.