# SoK: Arbitrage and Attack Strategies in Decentralized Finance (DeFi)

Hongzhi Liu
Dept. of Computer Science
ID:72403035

Qiulin Su
Dept. of Computer Science
ID:72405483

Xingyu Chen
Dept. of Computer Science
ID:72401656

Xinyue Liu
Dept. of Computer Science
ID:72403625

***Abstract*—Decentralized Finance (DeFi) has rapidly emerged as a transformative force in the blockchain ecosystem, enabling permissionless financial services through smart contracts. However, this innovation also introduces new risks, notably various forms of arbitrage and attack strategies that threaten the security and stability of DeFi protocols. This Systematization of Knowledge (SoK) paper provides a comprehensive survey and classification of arbitrage and attack techniques in DeFi. We systematically review the underlying mechanisms, present representative case studies, and analyze the impacts on the ecosystem. Furthermore, we discuss existing defense mechanisms, governance challenges, and outline open research directions. Our work aims to bridge the knowledge gap between academic research and industry practice, offering actionable insights for protocol designers, researchers, and regulators.**

***Index Terms*—Decentralized Finance, DeFi, Arbitrage, Attack, Blockchain, Smart Contract, Security, Systematization**

## I. Background and Preliminaries

### A. DeFi Primitives

Decentralized Finance (DeFi) systems are built upon a set of foundational primitives that serve as the core modules for constructing and composing more complex financial protocols [1]. Among these, smart contracts, tokens, oracles, keepers, and governance mechanisms are particularly essential to the operation and security of DeFi applications.

**Smart Contracts** are self-executing programs deployed on blockchains, which automatically enforce the rules and logic of financial agreements without the need for trusted intermediaries. They enable the creation of decentralized applications (dApps) and are the backbone of most DeFi protocols, ensuring transparency, automation, and tamper-resistance in financial transactions [1].

**Oracles** act as bridges between the blockchain and the external world, supplying smart contracts with off-chain data such as asset prices and real-world events. Since blockchains cannot natively access external information, oracles are critical for enabling a wide range of DeFi applications. The correctness and security of oracle data are vital, as manipulated or faulty inputs can introduce significant systemic risks to DeFi protocols [1].

**Keepers** are automated actors responsible for triggering on-chain actions either periodically or in response to specific conditions. For example, in lending protocols, keepers monitor the health of collateral positions and initiate liquidations when collateralization ratios fall below required thresholds. These roles can be fulfilled by any user or specialized bots, with incentive mechanisms in place to ensure the reliability and efficiency of protocol operations [1].

**Governance** mechanisms empower the community to make decisions regarding protocol parameters, upgrades, and resource allocation. Typically implemented through token-based voting, governance allows token holders to propose and vote on changes, thereby enabling the protocol to evolve and adapt in a decentralized manner. The design of governance systems directly impacts the security, adaptability, and responsiveness of DeFi protocols to community interests [1].

These primitives work in concert to provide the foundational infrastructure for the DeFi ecosystem. They ensure that protocols are automated, self-governing, and open, while also enabling further innovation and the composition of increasingly complex financial applications [1].

### B. DeFi Infrastructure and Core Protocols

The DeFi ecosystem is supported by a robust infrastructure and a diverse set of core protocols that facilitate decentralized financial activities. The foundational infrastructure includes public blockchains (e.g., Ethereum), decentralized identity management, and secure wallet solutions [2], [3]. On top of this infrastructure, several categories of core protocols have emerged as the backbone of DeFi.

**Automated Market Makers (AMMs):** AMMs have revolutionized decentralized trading by eliminating the need for order books and centralized market makers. Instead, they utilize liquidity pools and mathematical formulas to automatically determine asset prices and facilitate swaps [1].

**Lending Protocols:** Decentralized lending protocols enable users to lend and borrow digital assets in a permissionless manner. These protocols use smart contracts to manage collateral, calculate interest rates, and execute liquidations, thereby reducing counterparty risk [2].

**Stablecoin Protocols:** Stablecoins play a vital role in mitigating the volatility of cryptocurrencies by maintaining a stable value. These protocols employ various mechanisms, such as collateralization and algorithmic supply adjustments, to achieve price stability [2].

**Asset Management and Aggregators:** Asset management protocols offer yield optimization, automated portfolio management, and efficient routing of trades across multiple DeFi platforms [1].

Collectively, these core protocols provide the essential financial services—trading, lending, borrowing, and asset management—required for a functional and scalable DeFi ecosystem. Their composability further enables the creation of complex financial products and innovative applications, driving the rapid growth of decentralized finance [1], [2].

### C. Definitions and Distinctions: Arbitrage vs. Attack

Arbitrage and attack are two distinct yet sometimes overlapping forms of interaction with decentralized finance (DeFi) protocols [1], [4]. *Arbitrage* refers to the practice of exploiting price discrepancies across different markets or protocols to achieve risk-free profit. This activity is generally regarded as beneficial to the ecosystem, as it enhances price efficiency and market liquidity [2], [5]. For instance, arbitrageurs can synchronize asset prices between decentralized exchanges (DEXs) through atomic transactions.

In contrast, an *attack* is characterized by the deliberate exploitation of vulnerabilities or unintended behaviors within a protocol to extract value at the expense of other participants or the protocol itself [4]. Typical examples include oracle manipulation, reentrancy exploits, and governance attacks, which often result in financial losses or systemic instability [1], [2]. While both arbitrage and attacks may utilize similar technical tools—such as flash loans or composable contracts—their intent and impact are fundamentally different.

It is noteworthy that the boundary between arbitrage and attack can sometimes be ambiguous. Strategies such as sandwich attacks or frontrunning reside in a gray area, where profit is gained by exploiting information asymmetry or transaction ordering, sometimes at the expense of regular users [4]. As DeFi protocols evolve, differentiating between legitimate arbitrage and malicious exploitation remains a critical challenge for both researchers and protocol designers.

### D. Related Work

A substantial body of literature has been dedicated to the study of DeFi's security, economic incentives, and architectural properties. Werner et al. [1] present a comprehensive systematization of knowledge (SoK) on DeFi, covering protocol primitives, composability, and security aspects. Xu et al. [2] provide an in-depth analysis of DeFi security and privacy, identifying key vulnerabilities and attack vectors. Qin et al. [4] quantitatively analyze DeFi attacks, including arbitrage, frontrunning, and flash loan exploits, offering insights into the economic and technical drivers behind such incidents.

Other foundational works address specific protocol categories. Daian et al. [5] investigate the dual role of flash loans in enabling both arbitrage and attacks. Research on automated market makers (AMMs) [6] and decentralized oracle systems [7] further elucidates the trade-offs between efficiency, security, and decentralization in DeFi.

Collectively, these studies form the foundation for understanding the opportunities and risks inherent in DeFi, guiding the development of more secure and robust protocols.

### E. Comparison between DeFi and Traditional Finance

DeFi and traditional finance (TradFi) differ significantly in terms of system architecture, transparency, accessibility, risk profiles, and regulatory frameworks [1], [2].

**System Architecture and Intermediaries:** TradFi relies on centralized intermediaries such as banks, clearinghouses, and brokers to facilitate transactions and manage risks. In contrast, DeFi protocols operate on public blockchains and utilize smart contracts to automate financial services without trusted intermediaries, resulting in greater disintermediation and composability [2], [3].

**Transparency and Auditability:** DeFi systems offer high transparency, as all transactions and contract logic are publicly accessible on-chain, enabling real-time auditability [1]. TradFi systems, by contrast, are often opaque, with limited public visibility into internal operations.

**Accessibility and Inclusiveness:** DeFi provides global, permissionless access to financial services, lowering barriers for unbanked or underbanked populations. TradFi is subject to jurisdictional restrictions, KYC/AML requirements, and may exclude certain users due to regulatory or infrastructural constraints [2].

**Arbitrage Opportunities:** Both DeFi and TradFi present arbitrage opportunities, but the frequency and nature differ. DeFi's composability and atomic transactions enable rapid, on-chain arbitrage, often facilitated by flash loans [5]. In TradFi, arbitrage is limited by settlement times, regulatory oversight, and market fragmentation.

**Security Risks and Attack Surfaces:** DeFi introduces new attack vectors, including smart contract bugs, oracle manipulation, and economic exploits, which can be executed rapidly and globally [4]. TradFi, while still exposed to fraud and operational risk, benefits from established legal recourse and centralized monitoring.

**Regulatory Frameworks and Challenges:** TradFi operates within well-established regulatory frameworks, with oversight and compliance requirements. DeFi, by design, resists centralized control, posing significant challenges for regulation, enforcement, and consumer protection [1]. The decentralized and pseudonymous nature of DeFi complicates the application of traditional regulatory approaches.

In summary, while DeFi offers enhanced transparency, accessibility, and innovation, it also introduces unique risks and regulatory challenges absent in traditional financial systems. Understanding these distinctions is essential for both researchers and practitioners navigating the evolving landscape of decentralized finance.

## II. Systematization of Arbitrage Strategies

### A. Taxonomy and Theoretical Foundations

*1) Definition and Classification of Arbitrage in DeFi:* Arbitrage in Decentralized Finance (DeFi) refers to the systematic exploitation of price discrepancies for the same or similar assets across different DeFi protocols, markets, or trading pairs, with the objective of achieving risk-free or low-risk profits [8]. Unlike traditional finance, DeFi arbitrage is

enabled by the open, permissionless, and composable nature of blockchain-based protocols, which allows for atomic and programmable trading strategies.

We classify DeFi arbitrage into the following major categories:

- **Cross-Platform Arbitrage**: Exploiting price differences for a given asset across multiple decentralized exchanges (DEXs) or lending protocols.
- **Triangular Arbitrage**: Leveraging inconsistencies in exchange rates among three or more trading pairs within a single DEX or across multiple platforms.
- **Flash Loan Arbitrage**: Utilizing uncollateralized flash loans to conduct complex arbitrage strategies within a single atomic transaction, eliminating the need for upfront capital [9].
- **Oracle-Based Arbitrage**: Taking advantage of delays or inaccuracies in price oracles to execute profitable trades before the oracle updates are reflected across protocols.
- **Emerging Arbitrage Forms**: Including multi-chain arbitrage, cross-layer arbitrage, and miner extractable value (MEV)-based strategies, which exploit new composability and execution paradigms in DeFi [4].

Each category exhibits distinct operational mechanisms, risk profiles, and impacts on market efficiency and protocol security.

*2) Comparison with Traditional Finance Arbitrage:* While the fundamental principle of arbitrage—profiting from price discrepancies—remains unchanged, DeFi introduces several unique characteristics compared to traditional finance (TradFi) [1]:

- **Atomicity and Programmability**: DeFi arbitrage strategies can be executed atomically via smart contracts, ensuring that transactions either succeed entirely or fail without partial execution. This eliminates certain risks (e.g., execution risk) present in TradFi.
- **Permissionless Access**: Anyone with network access can participate in arbitrage, in contrast to TradFi where market access is often restricted by regulations or capital requirements.
- **Transparency and Composability**: All transactions and contract states are publicly visible and composable, enabling rapid strategy innovation but also increasing competition and adversarial behavior.
- **New Risk Vectors**: DeFi introduces protocol-specific risks such as smart contract vulnerabilities, oracle manipulation, and MEV, which are absent or less pronounced in TradFi [5].
- **Flash Loans**: The availability of flash loans—a DeFi-native primitive—allows arbitrageurs to access vast amounts of temporary liquidity without collateral, a capability not present in TradFi [9].

These differences fundamentally reshape the landscape of arbitrage, lowering barriers to entry while simultaneously increasing technical complexity and risk.

*3) Theoretical Models for DeFi Arbitrage:* The modeling of DeFi arbitrage builds upon and extends classical arbitrage theory from financial economics [10], while incorporating blockchain-specific features. Key theoretical frameworks include:

- **No-Arbitrage Principle in Automated Market Makers (AMMs)**: AMMs such as Uniswap maintain constant product or other invariant functions (e.g., $x \cdot y = k$), and arbitrageurs restore price equilibrium when deviations occur due to trades or liquidity shifts. Theoretical models analyze equilibrium conditions, slippage, and arbitrageur profit functions [6].
- **Game-Theoretic Models**: The open and competitive nature of DeFi arbitrage is amenable to game-theoretic analysis, modeling arbitrageurs as rational agents in a non-cooperative game, often under conditions of incomplete information and high competition [4].
- **MEV and Priority Gas Auction (PGA) Models**: Miner Extractable Value (MEV) introduces new strategic considerations, where arbitrageurs compete in gas auctions to prioritize their transactions, leading to models that analyze equilibrium bidding strategies and welfare implications [5].
- **Flash Loan Arbitrage Formalization**: Formal models capture the atomicity, capital efficiency, and risk-neutral properties of flash loan-enabled arbitrage, often using transaction graphs and state transition systems [9].

These theoretical models provide a foundation for understanding the efficiency, risks, and emergent behaviors in DeFi arbitrage, and guide both protocol design and risk management.

### *B. Cross-Platform Arbitrage: Mechanisms, Risks, and Ecosystem Impact*

*1) Mechanisms and Workflow:* Cross platform arbitrage, as one of the most mature arbitrage strategies in the DeFi ecosystem, focuses on capturing price differences between different trading platforms. The operation mechanism of this strategy is based on the transparency of blockchain and the programmability of smart contracts, and fully automated arbitrage operations are achieved through complex algorithms. The complete arbitrage workflow begins with real-time monitoring of market data, and professional arbitrage robots continuously scan dozens of DEX platforms on major public chains such as Ethereum and Binance Smart Chain, including mainstream protocols such as Uniswap, SushiSwap, Curve, etc. These monitoring systems use machine learning algorithms to process on chain data and can identify statistically significant price differences at the millisecond level.

When an arbitrage opportunity is detected, the system will immediately start the execution engine. Modern cross platform arbitrage typically adopts the ”atomic trading” model, which bundles trading operations from multiple platforms into the same blockchain transaction through smart contracts. This design ensures the atomicity of transactions: either all operations are successful or all are rolled back, completely eliminating some execution risks that exist in traditional financial markets. During the execution process, the arbitrage robot will dynamically calculate the optimal trading path, taking into account

factors such as the liquidity depth of each platform, trading fees, and real-time gas prices.

*2) Representative Case Studies:* The "stablecoin arbitrage" event that occurred in the summer of 2020 is a classic case of cross platform arbitrage. At that time, due to severe market fluctuations, DAI's trading price on the Curve platform remained 2-3 percentage points higher than other platforms. This price difference lasted for 72 hours, creating a rare opportunity for arbitrageurs to achieve stable returns. During this period, the professional arbitrage team accumulated profits exceeding $8 million, demonstrating the limitations of DeFi market efficiency and highlighting the positive role of arbitrage activities in market price discovery [11].

*3) Quantitative Analysis of Profitability and Risks:* According to research, Lightning Loan Arbitrage demonstrates the highest capital efficiency, with an average return rate of 300-800% per transaction. However, 32% of transactions fail due to smart contract vulnerabilities, reflecting the high-risk nature of high returns. In contrast, traditional cross platform arbitrage, although having lower returns, has a higher success rate and has become the most robust strategy choice.

In terms of risk adjusted returns, the Sharpe ratio of triangle arbitrage can reach 3.2, far higher than the arbitrage strategy in traditional financial markets. MEV competition has led to a 40-60% increase in transaction costs for ordinary users, resulting in significant negative externalities [12].

From the perspective of systemic risk, large-scale arbitrage trading involves an average of 3.2 jurisdictions and 5.7 DeFi protocols, forming a complex risk transmission network. It is particularly noteworthy that when market volatility exceeds the 30% threshold, arbitrage activities will suddenly decrease, leading to a brief expansion of price deviation [5].

### *C. Triangular Arbitrage: Principles and Real-World Implementations*

*1) Arbitrage Path Construction:* Triangle arbitrage, as a high-order arbitrage strategy in DeFi, focuses on utilizing the exchange rate imbalance between three or more assets to obtain risk-free profits. The identification of such arbitrage opportunities is essentially a graph theory problem, where nodes represent different cryptocurrency assets and edges represent exchange rate relationships between trading pairs. Modern arbitrage systems use an improved Bellman Ford algorithm to detect negative weight loops, which can effectively handle the high-frequency and low latency requirements unique to DeFi environments.

*2) Case Analysis: Successful and Failed Triangular Arbitrages:* The success and failure cases are as follows:

- **Successful Case:** The bZx attack demonstrated a profitable triangular arbitrage by exploiting price discrepancies across Uniswap, bZx, and Compound [11]. The attacker used flash loans to borrow ETH, artificially inflated WBTC's price on Uniswap locking in a profit of $\sim$1,193 ETH. The success relied on atomic execution, oracle manipulation, and minimal upfront capital [13].
- **Failed Case:** Not all arbitrage attempts succeed. For example, a trader identifying a 1% ETH $\rightarrow$ DAI $\rightarrow$ USDC $\rightarrow$ ETH arbitrage may fail due to slippage or front-running. High network congestion, impermanent loss in AMMs, and insufficient profit margins often render such strategies unviable. DEFIPOSER-ARB's greedy approach can also miss optimal paths if multiple arbitrage cycles exist [13].

*3) Market Efficiency and Impact:* The impact of triangular arbitrage activities on the efficiency of DeFi markets exhibits a clear duality.

- **Positive Impact:** Arbitrage behavior significantly improves price consistency between related trading pairs. Data shows that in active trading pairs of triangular arbitrage robots, the median price deviation has decreased from 0.8% to 0.15%, with an improvement of 81%. The additional trading volume brought by arbitrage trading increases the commission income of related liquidity pools by 35%–50%, objectively motivating more liquidity providers to participate in the market.
- **Negative Impact:** Intensive arbitrage trading exacerbates network congestion. Triangular arbitrage trading on the Ethereum mainnet once consumed 15% of the entire network's gas resources in a single day. [5] Competition between arbitrage robots leads to the "Race to the Bottom" phenomenon, where robots continuously raise gas prices to complete transactions earlier, resulting in 40%–60% of arbitrage profits being converted into miner income. This competition peaked in 2022, with some triangular arbitrage trades paying gas fees that exceeded the arbitrage profits themselves.

### *D. Flash Loan Arbitrage: Process, Case Studies, and Risk Assessment*

*1) Flash Loan Fundamentals and Protocols:* As a revolutionary financial tool in the DeFi field, Lightning Loan's core innovation lies in realizing an instant lending mechanism without collateral. This mechanism is based on the atomicity of blockchain transactions, allowing users to complete the entire process of "borrowing use repayment" within a single transaction [14]. At present, the mainstream lightning loan providers in the market include protocols such as Aave, dYdX, and Uniswap, which together form the lightning loan infrastructure of the DeFi ecosystem and provide basic support for various arbitrage strategies.

*2) Classic Flash Loan Arbitrage Cases:* The most famous example of DeFi's lightning loan arbitrage is undoubtedly the 2020 bZx protocol chain attack [11]. Attackers manipulate multiple DeFi protocol price oracle machines in a single transaction through intricately designed trading paths, ultimately achieving risk-free arbitrage. The attacker first borrowed 10000 ETH of Lightning Loan from dYdX, and then bought a large amount of sUSD on Uniswap, causing abnormal price fluctuations. They then used this manipulated price to open high leverage positions on the bZx platform, ultimately profiting over $1 million.

Another typical case is the flash loan arbitrage of PancakeSwap in 2021. Arbitrageurs used the price delay between Binance Smart Chain (BSC) and Ethereum mainnet to hedge transactions between the two markets through cross chain flash loans, with a single arbitrage yield of 3.5%. These cases not only demonstrate the technical complexity of Flash Loan arbitrage, but also expose the systemic risks brought by the combinatorial nature of DeFi protocols.

*3) Risk Factors and Systemic Implications:* Although flash loan arbitrage can create market efficiency, the systemic risks it brings cannot be ignored.

The primary risk comes from the security of smart contracts. Next is liquidity risk, as large-scale flash lending operations may instantly deplete the depth of the liquidity pool, leading to price slippage beyond expectations. The most serious risk is the systemic chain risk, as the high composability between DeFi protocols allows for the rapid transmission of individual protocol failures to the entire ecosystem through lightning lending operations. To address these risks, the industry is developing various mitigation measures, including introducing transaction delay mechanisms and improving oracle anti manipulation capabilities [11].

### *E. Oracle-Based Arbitrage and Manipulation*

*1) Oracle Mechanisms in DeFi:* The oracle system in decentralized finance serves as a critical infrastructure connecting on chain smart contracts and off chain data, and its design architecture directly affects the security of the entire ecosystem. The current mainstream oracle solutions are mainly divided into three categories: single source (such as Chainlink), multi-source aggregation (such as MakerDAO's OSM), and decentralized oracle networks (such as Band Protocol) [15].

*2) Arbitrage Strategies Leveraging Oracle Delays or Manipulation:* Professional arbitrageurs have developed various strategies that utilize the characteristics of oracle machines, among which the most typical is "time difference arbitrage". This strategy utilizes the time difference between price updates between different protocols for operation [15]. For example, when Chainlink updates the ETH price but MakerDAO's OSM has not yet been updated, arbitrageurs can conduct targeted trading on the protocol with price lag.

More complex strategies involve actively manipulating oracle inputs, such as creating artificial trading volumes on target DEX through lightning loans, affecting TWAP calculations, and then performing reverse operations on other protocols that rely on the oracle.

The "oracle game" strategy that emerged in 2023 is more aggressive. Arbitrageurs will monitor the clearing thresholds of major lending platforms. When they find that the price of a certain collateral is close to the clearing line, they will trigger clearing by artificially suppressing the spot market price, and then obtain assets at a discounted price.

*3) Case Studies and Defensive Measures:* The Alpha Finance incident in August 2021 is a typical case of oracle manipulation. The attacker manipulated the ETH price data of the Band Protocol oracle through lightning loans in a short period of time, and mortgaged a large amount of assets when the price was abnormally raised, ultimately causing a loss of $36 million. After analysis, it was found that the oracle system only relied on the middle price of 5 trading pairs and did not have sufficient outlier detection mechanisms [15].

The other is the Mango Markets attack, where attackers manipulated the price data of self built oracle machines to extract $117 million from the platform. The uniqueness of this case lies in the fact that the attacker legitimately exploited a design flaw in the custom oracle allowed by the protocol.

To address these threats, the industry has developed various defense measures. At the technical level, it includes introducing a multi-level data verification mechanism; At the economic level, security is enhanced by increasing node pledge requirements and setting punishment mechanisms; The latest development is the hybrid oracle system. However, completely eliminating oracle risks still faces fundamental challenges, especially in ensuring data timeliness while maintaining decentralization.

### *F. Emerging Arbitrage Innovations*

*1) Novel Strategies (e.g., Multi-chain, Cross-layer, MEV-based):* With the complex evolution of the DeFi ecosystem, arbitrage strategies are breaking through traditional paradigms and developing multiple innovative directions.

- **Multi-chain Arbitrage Strategy**: Profits by exploiting price differences between blockchain networks. In 2023, this became prominent through cross-chain stablecoin arbitrage (e.g., Ethereum-Arbitrum) using instant bridge transfers.
- **Cross-layer Arbitrage**: Utilizes information asymmetry between blockchain layers. A typical case is MEV arbitrage between Ethereum mainnet and Polygon zkEVM, where traders front-run pending Layer 2 transactions.
- **MEV-Driven Strategies**: The arbitrage strategy driven by MEV has developed into highly specialized sub sectors. In addition to traditional sandwich attacks, more innovative strategies include "Backrunning Arbitrage" - quickly executing subsequent arbitrage trades by analyzing the impact of confirmed trades on market conditions; And 'Bundle Arbitrage' - bundling multiple arbitrage opportunities into a single transaction and submitting it to validators [5].

*2) Theoretical and Practical Challenges:* These emerging arbitrage strategies face unprecedented theoretical challenges.

- **Theoretical Reconstruction**: The traditional no-arbitrage pricing theory requires redesign for multi-chain environments, incorporating cross-chain bridge latency and heterogeneous blockchain security. Game theory analysis becomes exponentially complex as arbitrageurs engage in multidimensional games with bridge operators and validators [9].
- **Practical Implementation Barriers**: Cross-layer arbitrage faces severe atomicity challenges in state consistency verification when operating across multiple

blockchain layers. The technical feasibility diminishes rapidly with increasing layer complexity.

- **Infrastructure Demands**: These strategies require sub-second latency for multi-chain status monitoring across dozens of blockchains [9]. MEV strategy R&D costs surge exponentially with advancing validator technology complexity.

### *G. Comparative Case Studies and Quantitative Impact Analysis*

TABLE I
ARBITRAGE STRATEGY RISK PROFILE

| Strategy | Key Risks |
|---|---|
| Cross-Platform Arbitrage | Front-running, Gas volatility |
| Triangular Arbitrage | Slippage accumulation, Path failure |
| Flash Loan Arbitrage | Contract vulnerabilities, Atomicity failure |
| Oracle Arbitrage | Data reliability, Regulatory risks |
| Cross-Chain Arbitrage | Cross-chain delay, Bridge risks |
| MEV-Driven Arbitrage | Validator collusion, Regulatory crackdown |

*1) Cross-Strategy Comparison Table:*

*2) Statistical Overview of Major Arbitrage Events:* Between 2020 and 2023, there have been several representative arbitrage events in the DeFi field, with significant differences in the performance of various strategy types

- **Cross-platform Arbitrage**: dominates in terms of the number of events, but the single profit is relatively small.
- **Flash Loan Arbitrage**: only accounts for a small number of events, it contributes a relatively high total profit [13].
- **Oracle Arbitrage**: the number of events is the smallest, but the average profit per transaction is high.
- **Emerging Strategies**:are showing explosive growth, with MEV related arbitrage accounting for 25% in 2023, an 8-fold increase from 2021. Although multi chain arbitrage has the lowest success rate, the average return rate of successful cases is 420%, demonstrating high-risk and high return characteristics.

*3) Impact on DeFi Ecosystem Stability:* Arbitrage activities have a dual impact on the stability of the DeFi ecosystem. Although high-frequency arbitrage improves market efficiency, it creates a "liquidity illusion" and quickly withdraws during market fluctuations. Arbitrage resulted in an annual loss of $730 million for liquidity providers, leading to a 40% decrease in retail LP participation. More seriously, the combination of protocols can trigger systemic risks, such as 68% of abnormal liquidation in the 2024 Aave liquidity crisis originating from cross protocol arbitrage chain reactions. However, moderate arbitrage can still help narrow price differentials and accelerate price discovery [5]. In the future, it is necessary to develop an intelligent regulatory system to distinguish between constructive and destructive arbitrage activities.

### *H. Summary and Research Gaps*

This chapter reveals the multidimensional characteristics of the DeFi arbitrage ecosystem, but there are still key gaps in current research: the lack of cross chain atomicity guarantees and secure proof of MEV democratization at the technical level; The economic model needs to reconstruct the multi chain pricing theory and deepen the research on the impact of liquidity; Regulatory science urgently needs to establish cross-border monitoring and MEV tax frameworks.

With the deepening integration of DeFi and traditional finance, it is necessary to build an integrated paradigm of cryptography, financial engineering, and regulatory technology through interdisciplinary collaboration in order to effectively balance the market efficiency improvement and systematic risk control of arbitrage activities.

## III. SYSTEMATIZATION OF ATTACK STRATEGIES

### *A. Taxonomy and Attack Models*

*1) Definition and Classification of Attacks in DeFi:* The definition and classification of attacks in Decentralized Finance (DeFi) are crucial for understanding the vulnerabilities inherent in DeFi protocols. This study categorizes DeFi attacks into two broad types: technical attacks and economic attacks. A structured methodology was followed, including the analysis of over 25 documented attack cases from 2020 to 2021 involving prominent DeFi protocols such as bZx, Harvest, Compound, and Cream Finance. The goal was to identify common patterns in these attacks and better understand their mechanics. Technical attacks are those that exploit specific vulnerabilities in the code or structure of a DeFi protocol, typically leading to immediate and risk-free gains for the attacker. These attacks often target smart contracts or exploit issues in transaction sequencing. For example, reentrancy attacks, where an attacker causes a contract to repeatedly call itself before updating its state, have been seen in attacks like the dForce hack (April 2020). Similarly, integer overflows and logic bugs can cause smart contracts to behave unexpectedly, resulting in significant financial losses for users or protocols. In contrast, economic attacks involve manipulating the broader financial incentives and market conditions over a longer period. These attacks are riskier, as they depend on the attacker's ability to predict or control market movements, but they can be highly profitable. Flash loans are a common tool in economic attacks, enabling attackers to borrow large amounts of capital for a very short period to manipulate prices or trigger arbitrage opportunities, such as in the Harvest protocol attack (October 2020). In these attacks, the attacker typically profits from the manipulation of assets and prices, exploiting the protocol's design flaws. The study further emphasizes the importance of addressing both technical vulnerabilities through tools like static analysis, formal verification, and economic vulnerabilities by designing better incentive structures. Misalignment of incentives, such as in governance or liquidity pools, often leads to significant risks, and these must be carefully managed to prevent malicious exploits.

*2) Attack Surfaces and Threat Models:* The analysis of attack surfaces and threat models in DeFi protocols reveals the main components that are vulnerable to exploitation.

These components include smart contracts, oracles, governance systems, transaction ordering mechanisms (such as Miner Extractable Value or MEV), and the composability of protocols. Each of these attack surfaces presents unique risks that require tailored mitigation strategies. Smart contracts are the most critical attack surface in DeFi, as they encode the logic of the protocols and handle the transfer of assets. Vulnerabilities in smart contracts, such as unprotected function calls or coding errors, can lead to significant losses. These risks can be mitigated by implementing reentrancy guards, formal verification, and static analysis tools. Ensuring the correctness of contract code and the integrity of state changes is vital for preventing exploits that manipulate contract logic. Oracles provide critical off-chain data, such as asset prices, to DeFi protocols. Because oracles typically rely on external data sources, they are vulnerable to manipulation, especially when market conditions are thin or when there is insufficient decentralization in the oracle design. Oracle manipulation attacks, such as altering price feeds to trigger liquidations or other financial events, can lead to significant losses for DeFi users. Mitigating these risks involves adopting decentralized oracles, using time-weighted average prices, and implementing stronger incentive structures for data integrity. Governance systems in DeFi protocols, which allow participants to vote on upgrades or changes to the protocol, present another key attack surface. Governance attacks, such as flash loan-based token accumulation or Governance Extractable Value (GEV) attacks, can allow malicious actors to seize control of the protocol and implement malicious upgrades. Mitigation strategies for these attacks include introducing voting delays, quorum thresholds, and optimistic veto systems to prevent a small group of actors from gaining disproportionate control. Transaction ordering, particularly in protocols that rely on automated market makers (AMMs), is another critical surface for attack. Front-running and sandwich attacks, where attackers manipulate transaction sequences to gain profit, are common threats. These attacks are often enabled by Miner Extractable Value (MEV), where miners or other participants can reorder transactions within a block for financial gain. Solutions to reduce the impact of MEV include private mempools and randomized transaction ordering to prevent attackers from predicting and exploiting transaction sequences. Finally, composability – the ability of different DeFi protocols to interact with one another – creates new vulnerabilities. A flaw in one protocol can trigger a cascading failure across multiple interconnected systems. For example, flash loans or other inter-protocol exploits can have outsized effects when protocols depend on one another for price feeds or collateral. To mitigate these risks, protocols should be stress-tested for composability vulnerabilities, and formal models of interdependencies should be developed to ensure robustness. In summary, the attack surfaces in DeFi protocols are varied, with each component presenting unique risks. Effective mitigation requires a combination of technical solutions, such as smart contract auditing and oracle decentralization, and economic measures, like incentive alignment and governance design. By addressing both the technical and economic vulnerabilities, DeFi protocols can better withstand malicious attacks and protect user funds.

### *B. Smart Contract Vulnerability Exploits*

*1) Common Vulnerabilities (Reentrancy, Overflow, Logic Bugs, etc.):* In order to identify and classify vulnerabilities in the Ethereum ecosystem, the study analyzed 40 known vulnerabilities, which were categorized across four major system layers: application, data, consensus, and network. These vulnerabilities were further evaluated based on:

Root causes (e.g., language-level flaws, protocol design) Potential for remediation (e.g., open, fixable, best-practice dependent) Impact on system-level properties: performance, security, and usability

Key evaluation metrics include flaws in Ethereum's architecture, its programming language Solidity, and the complexity inherent in decentralized blockchain environments.

Key Vulnerabilities: The study highlights several critical vulnerabilities affecting Ethereum, including:

Reentrancy (V1): One of the most infamous bugs, used in the 2016 DAO hack. Recursive calls allowed attackers to withdraw funds repeatedly before state updates.

Integer Overflow/Underflow (V6): A mathematical flaw due to missing boundary checks, leading to unexpected behavior and financial losses, as seen in the 2018 BEC Token attack.

Delegatecall Injection (V2): Enables the execution of arbitrary code within another contract's context. Exploited in the Parity Multisig Wallet attacks (2017).

Unprotected Suicide (V10): Contracts could be self-destructed without proper access control, permanently disabling associated functions.

tx.origin Misuse (V8): Misuse of `tx.origin` for authentication, allowing attackers to spoof trusted users.

Erroneous Visibility (V9): Functions intended to be private or internal were mistakenly exposed to public access, allowing unauthorized interactions.

Unchecked Call Return (V15): Failure to check return values from low-level external calls, leading to silent execution failures or unhandled logic errors.

These vulnerabilities highlight a fundamental issue in Ethereum's architecture: performance and security are deeply intertwined. For example, external calls not only increase gas usage but also introduce security risks. Many issues are specific to Ethereum due to its use of Solidity and the execution environment of the EVM. Furthermore, inadequate authentication, reliance on external dependencies, and poor development practices are identified as root contributors to many smart contract vulnerabilities.

*2) Representative Exploit Cases:* The analysis focused on prominent Ethereum exploit cases from 2016 to 2018, considering the financial losses incurred, the vulnerabilities exploited, and the attack vectors used. The study also documented the consequences of each incident, such as financial theft, denial of service (DoS), and permanent loss of access to contract functionality.

Selected Cases:

DAO Attack (2016) — *Loss:* $\sim$ *$60M*
Vulnerability: Reentrancy (V1)
Mechanism: Recursive calls to `splitDAO()` enabled attackers to repeatedly withdraw funds before state variables were updated.

Parity Multisig Wallet #1 (2017) — *Loss:* $\sim$ *$31M*
Vulnerabilities: Delegatecall Injection (V2), Erroneous Visibility (V9)
Mechanism: Attackers exploited improper fallback function visibility and a delegatecall injection to gain unauthorized access to wallet funds.

Parity Multisig Wallet #2 (2017) — *Funds Frozen:* $\sim$ *$280M*
Vulnerabilities: Frozen Ether (V3), Unprotected Suicide (V10)
Mechanism: A critical shared library contract was destructed, rendering all linked wallets inoperable and freezing their funds.

BEC Token Attack (2018) — *Estimated Loss: Unbounded Token Inflation*
Vulnerability: Integer Overflow (V6)
Mechanism: A multiplication overflow in the token contract enabled attackers to generate an arbitrarily large supply of tokens. Observations: Exploitation of Multiple Vulnerabilities: Several attacks leveraged a combination of vulnerabilities, such as the pairing of delegatecall misuse and faulty visibility in the Parity attacks. Neglect of Best Practices: Many of these exploits could have been prevented with proper authentication, visibility restrictions, and the use of libraries like `SafeMath` to prevent arithmetic errors.

*3) Quantitative Loss and Post-Mortem Analyses:* The study provided a quantitative analysis of the financial and security impacts of the examined attacks, categorized by vulnerability type and Ethereum system layer. It also involved a cross-layer mapping of attacks to the specific Ethereum components affected, such as the EVM, consensus protocol, and network infrastructure.

Insights: Severity of Application-Layer Attacks: Attacks targeting the application layer, particularly those exploiting smart contract vulnerabilities like reentrancy, caused the most significant financial losses. Interestingly, while these vulnerabilities caused major financial damage, the underlying Ethereum Virtual Machine (EVM) and host computers were not compromised due to their isolation.

Code Reuse Risks: Code-reuse in smart contracts, such as in the Parity Wallet incidents, introduced significant risks, highlighting the need for more robust auditing practices.

Ethereum's Security Limitations: Ethereum's permissionless nature allows anyone to interact with smart contracts, which, combined with immutability, makes it very difficult to patch vulnerabilities after deployment. This results in a substantial barrier to securing the platform post-incident.

Conclusion: The security of Ethereum is inherently complex due to its design and the programming language (Solidity), which introduces unique vulnerabilities that would not typically arise in traditional software development. The combination of high-profile attacks, many of which exploit smart contract vulnerabilities, demonstrates the urgent need for standardized security practices, robust auditing mechanisms, and a proactive approach to mitigating potential threats.

### C. Economic and MEV-Related Attacks

*1) Flash Loan Attacks: Beyond Arbitrage:* Flash loan attacks, particularly in the DeFi space, have emerged as a significant risk due to their ability to manipulate prices and exploit market inefficiencies. These attacks leverage the atomic nature of flash loans, enabling an attacker to borrow assets from a DeFi protocol without collateral, execute multiple trades across various platforms within a single transaction, and then repay the loan. This is done before the transaction can be reversed, making it a powerful tool for malicious actors.

The study adopts a data collection approach, where various high-profile flash loan attack incidents are analyzed. These attacks target vulnerabilities in price oracles, allowing attackers to manipulate asset prices and generate artificial profits, often from arbitrage opportunities. Tools like *FlashDeFier* are introduced to detect these price manipulation vulnerabilities, focusing on the static analysis of inter-contract data flow and utilizing taint analysis to trace malicious activities.

Key Findings: Flash loan attacks are not just limited to simple arbitrage, where an attacker seeks to profit from differences in token prices between different exchanges. They often exploit cross-contract dependencies—where a protocol's reliance on price oracles or the interaction between different smart contracts leads to vulnerability.

The research identified a 76.4% accuracy in detecting such attacks using *FlashDeFier*, which significantly outperformed earlier tools like *DeFiTainter*. This improvement highlights the growing complexity and sophistication of flash loan attacks, which go beyond simple arbitrage to include price manipulation and collateral-based exploits.

*2) Sandwich Attacks and Front-running:* Sandwich attacks and front-running are related techniques in the DeFi space that exploit transaction ordering. A sandwich attack typically involves placing a buy order before a target transaction (usually a large one) and then a sell order immediately after it, taking advantage of the price slippage caused by the large transaction. In contrast, front-running involves an attacker gaining prior knowledge of an incoming transaction and executing their own transaction before it, usually at a profit.

The methodology in studying these attacks includes monitoring transaction sequences within DeFi protocols, especially those using Automated Market Makers (AMMs) like Uniswap. The study evaluates how the mempool (transaction pool) is utilized to execute these attacks, analyzing their impact on the market price of assets and potential financial loss.

*3) Key Findings:* Both sandwich attacks and front-running are facilitated by Miner Extractable Value (MEV), where miners or validators can reorder transactions in the mempool to maximize their profits. By analyzing multiple instances of these attacks, the study highlights that such behaviors are often driven by incentive structures embedded within DeFi protocols.

For example, front-runners may manipulate transaction order to benefit from upcoming price movements, while sandwich attackers exploit slippage caused by large trades to profit from temporary price fluctuations.

The research suggests several mitigation strategies, including randomizing transaction ordering and using private transaction pools to reduce the transparency of transaction flows. Furthermore, addressing incentive misalignments in DeFi governance could reduce the motivations for such attacks and enhance protocol-level security.

*4) MEV Extraction Techniques and Their Impacts:* mev (miner extractable value) extraction techniques refer to the methods used by attackers or miners to capture value by reordering transactions in a blockchain. these techniques include sandwich attacks, front-running, and other transaction manipulation strategies. the study systematically maps mev extraction methods across various defi protocols, focusing on their economic impact and their consequences on liquidity providers and traders.

Evaluation metrics and methodology: key metrics for evaluating mev techniques include:

Transaction costs and execution slippage market impact and volatility profitability of attackers versus losses of honest participants system-wide factors such as blockchain throughput, latency, and scalability

The simulation models estimate the profitability of mev extraction under different blockchain configurations and protocol implementations.

key findings: mev extraction has far-reaching consequences beyond individual transactions. it contributes to market inefficiency, where malicious actors can manipulate prices, often at the expense of honest users. as mev activity increases, it creates disincentives for legitimate market participants and leads to centralization risks due to miner dominance in transaction ordering.

Mitigation strategies: the research suggests several countermeasures:

Algorithmic solutions such as *mev-boost*, which attempts to decentralize block production and reduce monopolistic control regulatory oversight to address incentive misalignments and promote fair trading practices transaction anonymization techniques, including private mempools, to limit front-running and reduce mempool transparency exploitation

*5) Case Studies and Statistical Losses:* Flash loan attacks, sandwich attacks, and MEV extraction techniques have emerged as significant threats to the DeFi ecosystem, with their combined financial losses reaching billions of dollars in recent years. These exploits typically leverage vulnerabilities in poorly designed price oracles, lack of transaction privacy, and weak governance models. The financial risks posed by these vulnerabilities are substantial, as attackers are able to manipulate prices, reorder transactions, and exploit governance systems for financial gain.

The most concerning aspect of these attacks is the systemic nature of their impact. The interconnectedness of DeFi protocols means that a vulnerability in one protocol can lead to cascading failures across others. For example, price oracle manipulation can distort asset values across multiple platforms, triggering automated liquidations or creating artificial price movements that can be exploited by attackers. Additionally, transaction privacy remains a critical issue, as front-running and sandwich attacks are enabled by the transparency of transaction ordering in public blockchains.

To address these challenges, there is a pressing need for more robust auditing mechanisms and enhanced security protocols within DeFi platforms. This includes the development of hybrid attack detection systems, which integrate both static and dynamic analysis tools to identify potential exploits before they are executed. The use of machine learning to predict and prevent new attack vectors is also a promising avenue, enabling protocols to adapt to emerging threats in real-time.

Another crucial aspect is the misalignment of incentives in DeFi governance. Malicious actors can exploit governance vulnerabilities, such as acquiring large amounts of tokens through flash loans to manipulate voting mechanisms. This highlights the need for stronger governance structures that balance power and ensure decisions are made in the protocol's best interest, rather than being driven by short-term financial gain.

Ultimately, addressing these security issues requires a comprehensive approach that includes privacy-enhancing technologies, such as private transaction pools, to reduce transaction ordering manipulation. Decentralized oracles and improved data accuracy can mitigate price manipulation risks, while economic reforms within governance models will help to prevent governance attacks. By strengthening these aspects, the DeFi ecosystem can become more secure, transparent, and resilient to future attacks.

### *D. Oracle Manipulation Attacks*

*1) Manipulation Techniques:* Manipulation techniques in DeFi protocols can be broadly categorized into two major types: price manipulation and transaction ordering manipulation. These attacks exploit weaknesses in how DeFi protocols obtain pricing data, typically through oracles, or how transactions are ordered within the blockchain. Price manipulation often involves exploiting vulnerabilities in oracle systems, which provide external data like asset prices to smart contracts. If oracles are compromised or unreliable, attackers can manipulate the data they feed into the system, triggering unintended outcomes like false liquidations or inflated prices that benefit the attacker.

Transaction ordering manipulation, such as front-running and sandwich attacks, allows attackers to profit by reordering transactions in a way that maximizes their own financial gains. This typically happens when an attacker can predict a large transaction and place their own orders before and after it, benefiting from the resulting price slippage. These techniques rely on the transparency of transaction ordering, where pending transactions are visible in the mempool, creating an opportunity for attackers to manipulate the sequence of events for personal gain.

These attacks are facilitated by the incentive structures inherent in DeFi protocols, especially the concept of Miner Extractable Value (MEV), which incentivizes miners to reorder transactions within a block to capture profits. The ability to exploit these systems with minimal capital—through tools like flash loans—amplifies the risk of manipulation, as attackers can borrow significant amounts of capital temporarily to execute large-scale manipulations without owning the assets.

Ensuring the security and reliability of oracles is critical to mitigating price manipulation. Without robust, decentralized oracles, price data can be easily tampered with, leading to significant financial losses for users and protocols. Moreover, improving transaction ordering systems, such as by implementing private transaction pools and randomized ordering, can help protect against front-running and sandwich attacks, making it harder for malicious actors to predict and exploit pending transactions.

*2) Notable Cases and Consequences:* Real-world DeFi attacks highlight the significant financial risks associated with vulnerabilities in smart contracts, oracles, and governance systems. The consequences of these attacks demonstrate how flaws in protocol design can lead to catastrophic financial losses and undermine trust in decentralized systems.

1. DAO Attack (2016): The DAO hack is a landmark example of a reentrancy vulnerability, where an attacker exploited the smart contract's failure to update its state before processing external calls. This allowed the attacker to repeatedly withdraw funds before they were recorded, draining $60 million from the DAO. The incident led to a hard fork in Ethereum, splitting the network into Ethereum (ETH) and Ethereum Classic (ETC), illustrating the profound impact that vulnerabilities in smart contracts can have on blockchain ecosystems.

2. Harvest Finance (2020): Attackers utilized flash loans to exploit price manipulation vulnerabilities in the oracles used by Harvest Finance. This allowed them to manipulate asset prices and drain $33.8 million from the protocol. The attack highlighted the risks posed by improperly secured price oracles, which are critical for DeFi protocols to function accurately. The ability to manipulate prices within DeFi systems not only resulted in significant financial loss but also damaged the reputation of the protocol and raised concerns about the security of similar protocols.

3. Ronin Bridge (2022): A more recent attack involved the Ronin Bridge, where a private key compromise allowed attackers to steal over $624 million. This exploit exposed the risks associated with centralized control over DeFi protocols, specifically the vulnerability introduced when critical infrastructure like key management is not sufficiently decentralized. The incident emphasized the need for secure key management practices and decentralized control mechanisms to prevent such high-value exploits.

These cases illustrate the risks inherent in DeFi, where the incentive structures, including miner rewards and transaction fees, can sometimes encourage actors to exploit vulnerabilities for financial gain. They also highlight a significant issue in DeFi protocols: the lack of standardized auditing and security measures. Without rigorous auditing, security gaps remain undetected until they are exploited, causing significant losses.

Oracles are integral to the functioning of DeFi, as they provide external data to smart contracts, enabling protocols to interact with real-world information, such as asset prices or interest rates. However, the reliance on these oracles introduces several security challenges that can have severe consequences for DeFi ecosystems.

1. Single Point of Failure: Many DeFi protocols rely on a single oracle for pricing data, creating a single point of failure. If the oracle is compromised, it can lead to erroneous data being fed into the system, causing widespread damage. For example, the Synthetix incident saw a $3 million loss due to incorrect oracle pricing, underscoring the risks associated with centralized oracles. These failures can cause forced liquidations at unfair prices, harming users and undermining confidence in the protocol.

2. Price Manipulation: Oracles are susceptible to manipulation, particularly when they rely on a limited number of data sources or lack decentralization. Attackers can manipulate the data provided by oracles, resulting in incorrect price feeds that trigger undesired automatic actions, such as liquidations or the creation of unstable assets. This vulnerability is especially dangerous in lending protocols, where incorrect price data can lead to significant financial losses, as seen in past attacks where manipulated prices led to unintentional liquidations of collateral.

3. Oracle Collusion: When multiple oracle providers collaborate or are compromised, they can collectively manipulate prices, affecting multiple DeFi protocols simultaneously. This type of attack is challenging to detect and defend against without a robust, decentralized oracle system. The reliance on a small set of data sources increases the likelihood of such collusion, making oracles a critical point of vulnerability in DeFi systems.

*3) Theoretical Limits of Oracle Security:* The theoretical limits of oracle security lie in the trade-off between decentralization and reliability. While decentralized oracles help mitigate single points of failure, they often suffer from lower accuracy and higher latency in price feeds, making them less reliable in fast-moving markets. Improving oracle security requires the development of more resilient systems that integrate multiple data sources, reduce the risk of manipulation, and ensure accurate and timely pricing.

Price manipulation, sandwich attacks, and MEV extraction represent critical vulnerabilities in the DeFi ecosystem, with significant implications for security and financial stability. The exploitation of oracle systems and transaction ordering mechanisms leads to substantial losses and can undermine the integrity of decentralized platforms. These vulnerabilities are often exacerbated by misaligned incentive structures and the lack of robust governance mechanisms.

To address these issues, there is an urgent need for more secure and decentralized oracles that can provide accurate price data and reduce the risk of manipulation. Additionally, improving transaction privacy through private mempools and

randomized ordering systems can mitigate the risks of front-running and sandwich attacks. Reforms in governance systems, such as introducing voting delays and quorum thresholds, are necessary to reduce the risk of governance exploits.

Incorporating secure auditing systems, automated testing frameworks, and machine learning models to predict and prevent attacks can help to fortify DeFi protocols against evolving threats. As the space continues to evolve, it will be crucial to adopt comprehensive security measures and establish industry standards to protect both users and protocols from the growing range of attacks targeting DeFi platforms.

### *E. Notable Cases, Loss Analysis, and Lessons Learned*

*1) Top Attack Incidents: Timeline and Loss Ranking:* DeFi protocols have been subjected to a significant number of security breaches, each with varying degrees of financial losses. These incidents, often driven by flaws in smart contracts, governance mechanisms, or economic models, have highlighted the critical need for more robust security frameworks within decentralized finance.

A clear pattern emerges from the timeline of attacks, with certain incidents being more impactful due to the type of vulnerability exploited and the resulting consequences. For instance, flash loan attacks have been among the most frequent, exploiting vulnerabilities in price oracles and liquidity pools. The Harvest Finance attack in 2020, which resulted in a loss of $33.8 million, is one of the most notable examples. In this attack, the price manipulation facilitated by flash loans allowed the attacker to exploit weaknesses in the integration of price oracles, leading to substantial financial losses. Another significant attack occurred with Cream Finance, where the attacker exploited vulnerabilities related to flash loans, resulting in a massive $130 million loss. This incident demonstrates the increasing sophistication of attackers, who target not just individual protocols but the very economic incentives within the DeFi ecosystem.

The DAO attack of 2016, which drained around $60 million, was another pivotal moment for DeFi security. It highlighted the risks of reentrancy attacks, where a smart contract's function allows an attacker to recursively withdraw funds before the system has updated its state. This attack set the precedent for the need for more rigorous testing and validation of smart contract functions before deployment.

Other major incidents, such as the Parity Multisig Wallet exploit in 2017, led to losses of $280 million due to vulnerabilities like unprotected suicide and delegatecall injection. These incidents emphasize how even slight oversights in smart contract design, especially in handling external interactions and function permissions, can lead to catastrophic consequences.

These examples show that the primary sources of DeFi security breaches involve weak or flawed contract logic, improper handling of user assets, and vulnerabilities in governance systems. As these attacks continue to evolve, they pose serious risks not only to individual users but also to the long-term sustainability of the DeFi space.

*2) Lessons for Protocol Designers:* From these high-profile incidents, several key lessons emerge for DeFi protocol designers aiming to enhance the security of their systems. First and foremost, a deep understanding of smart contract vulnerabilities is critical. Common issues like reentrancy, integer overflow, and oracle manipulation must be addressed with stringent testing and by implementing proven security measures like reentrancy guards and SafeMath libraries. Moreover, protocols should adopt formal verification techniques to ensure that the logic and execution of smart contracts are free from exploitable flaws before they are deployed.

Additionally, it is essential for designers to consider the incentive structures embedded within the protocols. Many of the attacks described above exploited economic vulnerabilities, such as price manipulation through flash loans or governance exploits through token accumulation. It is clear that incentive misalignments can drive attackers to exploit these systems for profit. To mitigate these risks, protocols must design incentives that align with the long-term security and stability of the system, incorporating anti-manipulation features and governance safeguards like voting delays and quorum requirements to prevent hostile takeovers via governance mechanisms.

Another major takeaway is the importance of composability in DeFi protocols. While composability allows different protocols to interact and create more complex financial products, it also amplifies risks. A vulnerability in one protocol can cascade across the entire ecosystem, triggering a chain reaction of failures. Therefore, stress testing and simulation tools are critical to evaluate how interconnected protocols will behave under extreme conditions. Furthermore, the use of decentralized oracles with proper data validation mechanisms can help protect against price manipulation, which remains a significant attack vector in the DeFi space.

Lastly, monitoring and incident response strategies need to be established. Protocols should not only focus on preventing attacks but also prepare for rapid responses in the event of a breach. Continuous monitoring, along with real-time auditing and security updates, can help identify emerging threats and mitigate losses.

In conclusion, securing DeFi protocols requires a multifaceted approach that considers both technical vulnerabilities and economic incentives. By integrating strong security practices, enhancing governance models, and considering the broader systemic impacts of composability and external data reliance, designers can help fortify their protocols against the increasingly sophisticated attacks that continue to target the DeFi ecosystem.

### *F. Summary and Open Challenges*

Decentralized Finance (DeFi) has introduced innovative financial models, but it has also created a complex environment that is highly susceptible to various types of attacks. A systematic understanding of these attacks is crucial to safeguarding the ecosystem. The most prominent attack strategies involve technical attacks, which target vulnerabilities in smart contract code, and economic attacks, where market conditions

or governance structures are manipulated for malicious gain. Tools such as flash loans, reentrancy vulnerabilities, and oracle price manipulation are often leveraged to carry out these attacks, exploiting the open and transparent nature of DeFi systems.

Smart contracts are a primary attack surface due to their role in automating transactions and managing funds. Vulnerabilities such as coding errors or logic flaws can have severe financial implications. Oracles, which provide real-time data for smart contracts, are another critical vulnerability. Attackers can manipulate these oracles, causing incorrect data to be fed into the system and triggering events like forced liquidations or distorted prices. The issue of Miner Extractable Value (MEV), where attackers profit by manipulating transaction ordering, is another challenge that destabilizes decentralized exchanges (DEXs) and creates unfair market conditions.

Despite improvements in detecting and mitigating such risks—through tools like FlashDeFier for detecting flash loan attacks and formal verification processes for smart contracts—there are still gaps in security practices across the DeFi space. These gaps result in fragmented efforts to address vulnerabilities, which leave protocols exposed. Privacy-enhancing technologies, which could reduce issues like front-running and MEV extraction, are still in early development and face challenges related to scalability and integration with existing protocols.

Governance systems and incentive misalignment are significant risks in DeFi. Malicious actors can exploit weak governance models, especially through methods like flash loan manipulation, allowing them to gain control over protocols and enact harmful changes. Solutions to address these governance vulnerabilities are complex, requiring a balance between decentralization and security to ensure that decision-making power is distributed but still protected from manipulation.

The inherent composability of DeFi protocols also adds a layer of risk. The interconnectedness of protocols means that vulnerabilities in one can cascade and affect multiple systems. This interconnectedness amplifies the potential impact of an attack. To mitigate these risks, stress testing and formalizing inter-protocol dependencies are necessary to assess the potential for system-wide failures.

Key open challenges include the need for comprehensive frameworks to detect and address complex attacks, improving the scalability of privacy solutions, resolving governance issues, and establishing standardized cross-protocol security measures. As DeFi protocols continue to evolve, constant innovation in attack detection tools, economic incentive models, and security frameworks will be essential to maintain the integrity and trustworthiness of DeFi ecosystems.

In conclusion, while DeFi has the potential to revolutionize finance, ensuring its security requires a holistic approach that considers both technical vulnerabilities and economic incentives. Tackling the open challenges—improving privacy solutions, enhancing governance models, and implementing stronger attack detection measures—will be crucial for the sustainability and long-term success of the DeFi ecosystem.

## IV. Defense Mechanisms and Governance

### A. Technical Defenses

*1) Smart Contract Audits and Formal Verification:* Smart contract audits and formal verification represent the first line of defense against vulnerabilities in DeFi protocols. Audits involve comprehensive code reviews by security experts to identify potential vulnerabilities before deployment. According to Chen et al. [16], professional audit firms typically employ a multi-layered approach including manual code review, automated tool scanning, and simulation of attack scenarios.

Formal verification, in contrast, provides mathematical proof of a contract's correctness with respect to a formal specification. As Wu et al. [17] note, "formal verification can be divided into static symbolic execution and dynamic symbolic execution," with each approach offering different security guarantees. Static methods analyze code without execution, while dynamic methods observe runtime behavior.

Recent advancements have seen the integration of both approaches. For example, tools like Securify combine techniques by splitting smart contracts into independent parts for verification, thereby "improving the degree of automation" and addressing the path space explosion problem common in formal verification [17].

Despite their effectiveness, these approaches face limitations. Ince et al. [18] observe that "while these tools show promise, they are not ready to replace more traditional manual reviews," highlighting that complete security remains a combination of automated and human expertise.

*2) Oracle Security Enhancements:* Oracles represent a critical vulnerability point in DeFi systems as they connect on-chain smart contracts with off-chain data. According to Werner et al. [1], insecure oracles have contributed to some of the largest DeFi exploits in history.

Several technical solutions have emerged to enhance oracle security:

- **Multiple Data Sources**: Using a diversity of oracles through an M-of-N reporter mechanism, where price feeds are aggregated from multiple providers. This approach calculates the median price and ignores outliers that deviate significantly from the consensus [17].
- **Time-Weighted Average Price (TWAP)**: Protocols like Uniswap V2 implement TWAP mechanisms that track prices over time, making manipulation more difficult and expensive. This reduces the risk of flash loan attacks by requiring sustained price manipulation rather than momentary spikes [19].
- **Circuit Breakers**: Implementation of price deviation limits that temporarily halt trading when prices move beyond predefined thresholds. This provides time for human verification and prevents catastrophic losses during price manipulation attempts.
- **Cryptographic Verification**: Advanced oracle systems like Chainlink employ cryptographic proofs to verify data integrity and source authenticity, significantly raising the bar for attackers [1].

The effectiveness of these measures varies by implementation. Cole [20] notes that "oracles using multiple sources and robust verification can reduce the attack surface, but complete security requires continuous evolution of defensive measures."

*3) MEV Mitigation Techniques:* Miner Extractable Value (MEV) represents a significant threat to DeFi users through transaction reordering, frontrunning, and sandwich attacks. Various technical solutions have been developed to mitigate these risks:

- **Commit-Reveal Schemes**: These protocols require users to commit to transactions without revealing details, then exposing them only after the commitment is recorded on-chain, preventing frontrunning [5].
- **Timelock Delays**: Implementing mandatory waiting periods between transaction submission and execution, reducing the opportunity for MEV extraction [4].
- **Fair Sequencing Services**: Protocols like Chainlink's Fair Sequencing Service and Ethereum's proposed MEV-Boost aim to create fair ordering mechanisms that prevent miners from arbitrarily reordering transactions for profit.
- **Privacy-Preserving Transactions**: Solutions like Aztec Protocol and zk-rollups that shield transaction details until execution, preventing MEV extractors from identifying profitable opportunities [21].

As noted by Heimbach and Wattenhofer [22], "eliminating sandwich attacks requires game-theoretic approaches that align incentives across the ecosystem," showing that technical solutions must be complemented by economic design considerations.

*4) Case Studies: Defense Successes and Failures:* Analysis of real-world incidents provides valuable insights into the effectiveness of technical defenses:

**Success Case: MakerDAO Resilience**

MakerDAO's robust defense mechanisms were tested during the March 2020 market crash. Despite extreme market volatility, its multi-layered defenses including price delay mechanisms, emergency shutdown capabilities, and governance-controlled risk parameters allowed the protocol to survive without completely collapsing [2].

As Cole [20] observes, "previous audits had identified potential risks in reserve composition, allowing for faster response and recovery during the incident." This highlights how proactive security measures provided resilience during crisis scenarios.

**Failure Case: Wormhole Bridge Exploit**

In February 2022, the Wormhole bridge between Ethereum and Solana was exploited for 120,000 ETH (approximately $325 million at the time). The attack succeeded because developers had enabled a deprecated function that allowed forged signatures to be verified, bypassing critical security checks [17].

This case demonstrates that even after formal verification and audits, operational security remains critical. The vulnerability occurred not in the core logic but in a deprecated function that remained accessible, highlighting the importance of comprehensive security review and proper deprecation procedures.

### *B. Economic Incentives and Mechanism Design*

*1) Incentive-Compatible Security Models:* DeFi protocols increasingly employ economic mechanisms to align participant incentives with protocol security. These approaches recognize that technical safeguards alone cannot ensure security without appropriate economic design.

The concept of "economic security" suggests that protocols should be designed such that rational actors find attacking the system more costly than operating within its rules. This approach relies on quantifying attack costs against potential profits, creating systems where security violations are economically irrational [19].

Key incentive-compatible security models include:

- **Stake-Based Security**: Requiring validators, liquidity providers, or other participants to lock collateral that can be slashed for malicious behavior. This creates "skin in the game" that disincentivizes attacks.
- **Fee Structures**: Implementing transaction fees that increase during periods of high volatility or congestion, making certain attack vectors prohibitively expensive during vulnerable times.
- **Reward Distribution**: Designing token reward mechanisms that encourage long-term participation and protocol health rather than short-term exploitation. This can include vesting schedules and participation multipliers.

Werner et al. [1] note that "incentive-compatible designs must account for rational behavior under imperfect information," highlighting the need for models that remain secure even when participants have asymmetric information or bounded rationality.

*2) Game-Theoretic Approaches:* Game theory provides a mathematical framework for analyzing strategic interactions between rational actors in DeFi ecosystems. Several game-theoretic models have been applied to strengthen protocol security:

- **Nash Equilibrium Analysis**: Designing protocols where the Nash equilibrium (where no participant benefits from changing strategy unilaterally) aligns with desired security properties. This creates self-enforcing security without requiring trust [4].
- **Schelling Points**: Creating focal points where participants naturally converge on secure behaviors through common knowledge and expectations, even without communication.
- **Signaling Games**: Implementing mechanisms where honest participants can credibly signal their trustworthiness, allowing protocols to distinguish between honest and potentially malicious actors.

Daian et al. [5] demonstrate how game theory can be applied to the MEV problem, modeling priority gas auctions as non-cooperative games and analyzing equilibrium bidding strategies. Their work shows that "without proper mechanism

design, competitive equilibria often lead to wasteful outcomes" such as elevated gas prices and network congestion.

*3) Case Analysis: Effective Economic Defenses:* **Maker Protocol Liquidation System**

The Maker Protocol's liquidation mechanism exemplifies effective economic defense design. Liquidators (called "keepers") are incentivized to monitor collateralized debt positions and liquidate undercollateralized loans. The protocol offers a liquidation discount that makes this behavior profitable while protecting the system from insolvency.

During the March 2020 market crash, this system came under extreme stress but ultimately functioned as designed. While some auctions cleared at zero bids due to gas price spikes and market congestion, the subsequent governance response implemented improvements including Dutch auction mechanisms and circuit breakers [1].

**Curve Finance Vote-Escrowed Tokenomics**

Curve Finance introduced vote-escrowed CRV (veCRV), requiring users to lock their CRV tokens for extended periods to gain governance rights and boosted rewards. This mechanism creates strong economic incentives for long-term participation and alignment with protocol health.

As Cole [20] observes, this design "strengthens user trust and adoption through regular security updates, community involvement in governance, and transparent vulnerability disclosure," demonstrating how economic incentives can enhance protocol security and stability.

### *C. Community Governance and Incident Response*

*1) DAO-based Governance Mechanisms:* Decentralized Autonomous Organizations (DAOs) represent the primary governance structure for managing DeFi protocols. These governance systems enable token holders to propose and vote on changes to protocol parameters, security measures, and resource allocation.

Effective DAO governance mechanisms typically include:

- **Multi-tiered Proposal Systems**: Structured processes where proposals must pass through discussion, formal submission, and voting phases before implementation. This creates deliberative checks against harmful changes.
- **Delegation**: Allowing token holders to delegate their voting power to technically proficient community members who may better understand complex security implications.
- **Time-Delayed Execution**: Implementing mandatory waiting periods between approval and execution of governance decisions, providing time for security review and emergency response if necessary.
- **Specialized Security Councils**: Creating dedicated groups with expertise in security to review protocol changes and respond to emergencies, sometimes with special powers to implement time-sensitive security fixes.

As noted by Xu et al. [2], "the design of governance systems directly impacts the security, adaptability, and responsiveness of DeFi protocols to community interests." However, governance itself can become an attack vector if not properly secured.

*2) Incident Response and Recovery Case Studies:* **Compound Finance Oracle Error (November 2021)**

In November 2021, Compound Finance experienced an incident where a buggy price feed allowed users to borrow assets against inflated collateral values. The community response demonstrated both strengths and weaknesses of decentralized governance:

The immediate response included identifying the issue, communicating with users, and developing a technical fix. However, the governance process required multiple days to pass and implement the solution due to mandatory timelock delays. This highlights the tension between security-focused time delays and responsive incident management.

**Wormhole Bridge Recovery (February 2022)**

Following the $325 million Wormhole bridge exploit, Jump Crypto (the parent company of Wormhole) stepped in to replenish the stolen funds, preventing ecosystem collapse. This case demonstrates the hybrid nature of many DeFi recovery processes, where centralized entities often play crucial roles despite decentralized governance structures.

As Wu et al. [17] note, the recovery involved "operational error response" highlighting that incident response frameworks must account for both technical and human factors in recovery planning.

*3) Challenges in Decentralized Coordination:* Decentralized governance faces several coordination challenges that affect security incident response:

- **Response Speed vs. Deliberation**: The inherent tension between rapid response to security incidents and thorough community deliberation. Time-sensitive vulnerabilities may require action faster than governance processes allow.
- **Information Asymmetry**: Varying levels of technical expertise among governance participants can lead to difficulty evaluating complex security proposals or understanding vulnerability implications.
- **Voter Participation**: Low participation rates in governance votes may result in decisions made by small, potentially non-representative groups of token holders.
- **Cross-Protocol Coordination**: Security incidents often affect multiple interconnected protocols, requiring coordination across different governance systems with varying processes and timelines.

Werner et al. [1] observe that "decentralized governance mechanisms must balance security, nimbleness, and inclusivity" to effectively respond to evolving threats while maintaining community alignment.

### *D. Limitations and Challenges*

*1) Technical, Economic, and Social Limitations:* **Technical Limitations**:

- **Formal Verification Boundaries**: Even formally verified contracts may contain vulnerabilities if the specifications themselves are flawed or incomplete. As Chen et al. [21]

note, "formal verification cannot guarantee the absence of all vulnerabilities, only conformance to specified properties."

- **Oracle Constraints**: Complete decentralization of oracle systems remains challenging, creating points of centralization within otherwise decentralized systems.
- **Composability Risks**: The interoperability of DeFi protocols creates complex interaction surfaces that are difficult to fully secure. Security guarantees for individual protocols may break down when they interact in unexpected ways.

**Economic Limitations**:

- **Capital Efficiency vs. Security**: Security measures often reduce capital efficiency, creating competitive disadvantages for more secure protocols in the short term.
- **MEV Persistence**: Despite mitigation efforts, MEV extraction continues to evolve, with extractors developing increasingly sophisticated techniques that exploit new vulnerabilities.
- **Incentive Misalignment**: Token distribution and governance structures may create misaligned incentives between short-term token holders and long-term protocol health.

**Social Limitations**:

- **Governance Capture**: Concentration of governance tokens can lead to plutocratic control, potentially undermining decentralization principles.
- **Technical Barriers**: Complex security mechanisms may exclude less technical participants from effective governance participation.
- **Regulatory Uncertainty**: The evolving regulatory landscape creates uncertainty for protocol developers implementing security measures.

*2) Open Problems:* Several critical challenges remain unsolved in DeFi security:

- **Cross-Chain Security**: As DeFi expands across multiple blockchains, securing cross-chain bridges and interactions presents unique challenges not fully addressed by current security models.
- **Scaling Security Solutions**: Ensuring that security mechanisms can scale with growing protocol adoption and increasing transaction volumes.
- **Privacy vs. Transparency**: Balancing the transparency needed for security analysis with privacy requirements for users and competitive protocol operations.
- **Economic Sustainability of Security**: Developing sustainable funding models for ongoing security research, audits, and incident response capabilities.
- **Standardization**: Creating common security standards and best practices across the ecosystem while allowing for protocol-specific innovation.

Salzano et al. [23] identify "gaps between academic literature and practical development" in addressing security vulnerabilities, particularly in areas such as denial of service, bad randomness, and time manipulation, where developer practices often diverge from academic recommendations.

### *E. Summary*

DeFi defense mechanisms have evolved significantly, combining technical safeguards, economic incentives, and governance processes to create multi-layered security systems. Technical defenses including formal verification, oracle enhancements, and MEV mitigation provide foundational security, while economic mechanism design aligns participant incentives with protocol security. Community governance systems enable adaptive response to emerging threats and coordinate recovery efforts when incidents occur.

Despite these advances, significant challenges remain. The composable nature of DeFi creates complex attack surfaces that are difficult to fully secure, while tensions between capital efficiency, usability, and security create ongoing tradeoffs. Governance systems continue to struggle with balancing responsive decision-making against inclusive deliberation.

The most promising approaches integrate multiple defense layers, recognizing that no single security mechanism is sufficient. As Werner et al. [1] conclude, "the robustness of DeFi protocols depends not only on technical implementation but on the alignment of economic incentives and effective governance." This holistic approach acknowledges that security emerges from the interaction between code, economics, and community, requiring continuous evolution as the threat landscape changes.

Future research and development should focus on addressing the identified open problems, particularly cross-chain security, scalable security solutions, and sustainable economic models for security funding. Standardization efforts may help establish common security baselines while allowing for protocol-specific innovation, bridging the gap between academic research and developer practices identified by Salzano et al. [23].

## V. Discussion and Future Directions

### *A. The Grey Area Between Arbitrage and Attack*

*1) Case Studies: Ethical and Legal Ambiguities:* In the DeFi field, the boundary between arbitrage and attack is often blurred.

- In the Poly Network attack, the attacker exploited and stole assets, ultimately earning a $500000 vulnerability bounty and retaining the title of "Chief Security Advisor" granted by the project team. This incident has sparked a heated debate about the standard of 'ethical hacking', which could set a dangerous precedent by legitimizing theft [1].
- In the Mango Markets incident, attackers profited by manipulating oracle prices and cited protocol autonomy rules to defend themselves, exposing a fatal flaw in DeFi governance mechanisms: the lack of an authoritative arbitration framework when technical feasibility, community governance, and legal norms conflict [9].

- From an ethical perspective, the universalization of Sandwich Attack has sparked deeper thinking. About 23% of MEV profits on Ethereum in 2023 come from this strategy that harms the interests of ordinary users, and when participants are informed that their arbitrage behavior will result in losses for others, 78% still choose to continue executing it, reflecting the role of DeFi anonymity in dissolving ethical constraints [1]. What's even more tricky is that such strategies are often in a gray area of the existing legal system - they strictly follow protocol rules but clearly violate fair trade principles.

*2) Regulatory and Governance Implications:* These peripheral cases pose unprecedented challenges to regulatory frameworks.

- In the first DeFi enforcement guidelines released by the US SEC in October 2023, it was explicitly included for the first time in the category of securities fraud that "the use of technological advantages to obtain unfair benefits" was included. But the guide has faced strong opposition from the crypto community, who believe it fails to distinguish the core differences between innovative arbitrage and fraudulent behavior.
- In terms of governance mechanisms, DAO organizations are exploring new solutions. The "MEV Recovery Pool" mechanism introduced by Uniswap in 2023 is quite innovative, capturing a portion of arbitrage profits through the protocol layer and returning them to liquidity providers. After the implementation of this mechanism, the number of related controversial proposals has decreased [1].
- From an international coordination perspective, the Financial Stability Board (FSB) 2023 report points out that regulatory differences among countries regarding DeFi arbitrage may lead to serious regulatory arbitrage. Establishing a globally unified classification standard has become a priority agenda for international organizations.

These developments indicate that DeFi governance is entering a new stage of tripartite synergy of "technology+law+ethics".

### *B. Future Trends in the DeFi Ecosystem*

*1) Technological Innovations :*

- **AI**: Artificial intelligence and machine learning are reshaping the competitive landscape of DeFi arbitrage strategies. In the fourth quarter of 2023, the first batch of arbitrage robots based on GPT-4 will use natural language processing capabilities to analyze news events and social media emotions in real time, increasing the response speed of event driven arbitrage to three times that of traditional systems. In the path optimization of reinforcement learning, AI models can autonomously discover arbitrage patterns that human developers have not recognized by simulating millions of historical trading scenarios, and increase the triangular arbitrage yield by 40% in backtesting.
- **Layer 2**: The Layer 2 solution is creating a new paradigm for arbitrage strategies. Arbitrarum Nova's "AnyTrust" mechanism and Optimism's "Bedrock" upgrade have compressed the time window for cross layer arbitrage from the original 12-15 seconds to 3 seconds. This has led to the basic exit of traditional manual arbitrage from the market, and the dominance of "ultra-low latency systems" developed by professional institutions.
- **Cross-chain**: The evolution of cross chain technology is rewriting the risk return ratio of multi chain arbitrage. Based on the Cosmos IBC and LayerZero atomic exchange protocol, the success rate of cross chain arbitrage has been increased from less than 20% in the early days to 68%. However, these advances are also accompanied by new security risks, and cross chain bridges have become the primary target of hacker attacks [1].

*2) Regulatory Evolution and Global Trends:* The global regulatory framework is undergoing a critical period of transformation.

The DeFi Market Regulation, passed by the US SEC in March 2024, pioneered the use of the "substance over form" principle to include eligible arbitrage activities in securities trading regulation. The European Union, on the other hand, passed secondary legislation under the MiCA regulation, requiring all "professional arbitrageurs" to register and pay trading margins, and violators will face a fine of 10% of annual turnover.

Developing countries are forming distinctive regulatory pathways. India's "sandbox regulation" program allows testing high-risk arbitrage strategies, but requires 20% of profits to be deposited into regulatory insurance funds. The "Digital Asset Market Maker License" launched by the Central Bank of Nigeria has integrated arbitrage institutions into the formal financial system, bringing the country's stablecoin arbitrage spread down from 3% to 0.5%.

### *C. Emerging Challenges for Research and Industry*

*1) Scalability, Privacy, and Composability:*

- **Scalability**: The scalability bottleneck has become the primary obstacle to the development of DeFi arbitrage strategies. Professional arbitrage robots contribute 32% of the trading volume on the entire network, but only gain 15% of the block space. When TPS exceeds 2000, the existing MEV auction mechanism completely collapses, resulting in the phenomenon of "arbitrage black hole" - high-value arbitrage opportunities cannot be captured due to network congestion [1].
- **Privacy**: The fundamental conflict between privacy protection requirements and regulatory transparency requirements. The "zk arbitrage" protocol developed by the Zcash Foundation in 2023, although capable of hiding trading paths, has been strongly warned by the FATF that it violates "travel rules".
- **Composability**: The composability risk increases exponentially with the complexity of the protocol. When the depth of smart contract calls exceeds 7 layers, the probability of unexpected combination behavior is as high as 43%. The "composite clearing storm" that occurred in

March 2024 is a typical case: a conventional ETH price fluctuation triggered 68% of erroneous abnormal clearing through a chain reaction of 11 protocols, and existing security tools are simply unable to detect such "cross protocol cascading effects" [1].

*2) Interdisciplinary Research Opportunities:* The combination of behavioral finance and DeFi arbitrage has opened up a new research paradigm. The 2024 experiment conducted by the Centre for Emerging Finance at the University of Cambridge revealed that when the arbitrage interface incorporates the "social loss visualization" feature, 42% of participants will voluntarily give up up up up to 30% of profit opportunities. This phenomenon of "on chain altruism" completely overturns the rational assumption of traditional finance.

The climate finance perspective is reshaping the evaluation criteria for arbitrage infrastructure. According to calculations by the Carbon Chain Think Tank, the energy consumed by a typical sandwich attack on Ethereum was equivalent to the daily electricity consumption of 30 American households, and the annual carbon footprint of the entire DeFi arbitrage ecosystem has exceeded that of Iceland, which has spurred innovation in "green arbitrage" [5].

Complex systems science provides new tools for risk management. The project between Santa Fe Institute and MakerDAO is the first to apply the resilience theory of ecosystems to DeFi stress testing. They found that arbitrage activities actually established a "financial contagion channel" between protocols, and its network topology features were remarkably similar to the spread of epidemics. The 'risk propagation model' developed based on this has successfully predicted the Aave liquidity crisis in January 2024, issuing a warning 72 hours in advance.

### D. Open Research Directions

*1) Key Open Questions:* The atomic problem of cross protocol arbitrage remains the most pressing unresolved challenge in the DeFi field. There is currently no solution that can truly guarantee atomic execution of complex arbitrage trades involving three or more protocols. The core challenge lies in designing a universal atomic framework when some protocols adopt deterministic consensus while others use probabilistic consensus [5].

The impact mechanism of dynamic cost markets on arbitrage strategies urgently needs to be further studied. After the implementation of EIP-7623 in 2024, the volatility of Ethereum base fees increased fourfold, but the adaptation strategies of arbitrage robots showed puzzling differentiation. This bimodal distribution violates the predictions of traditional auction theory and implies the existence of deeper game equilibrium.

The framework for long-term ecological impact assessment is completely lacking. All current arbitrage research focuses on short-term market impacts, but the DeFi protocol, as a characteristic of "programmable currency Lego," may lead to profound systemic restructuring of arbitrage activities.

*2) Suggested Methodologies and Approaches:* Large scale multi-agent simulation should become a fundamental research tool. Unlike traditional financial research, DeFi arbitrage involves real-time interactions among hundreds of heterogeneous agents. The simulation results of the "DeFiSim" platform developed by the University of Berkeley show that certain arbitrage strategies can generate network effects similar to quantum entanglement. This method is particularly suitable for studying emerging cross chain MEV problems. By constructing a virtual cross chain environment, potential arbitrage crisis points can be identified in advance [1].

The construction of interdisciplinary knowledge graphs is crucial for understanding complex influences. The "DeFi Cognitive Graph" project launched by the University of Cambridge systematically models for the first time the four-dimensional effects of arbitrage activities on technology stacks, economic models, legal frameworks, and social impacts.

Quantum computing experiments should be planned in advance. Although current quantum computers are unable to handle DeFi problems on a practical scale, transforming arbitrage opportunity recognition into quantum support vector machine (QSVM) problems theoretically allows for the completion of tasks that traditional computers require polynomial time to solve in logarithmic time. This exponential acceleration may completely change the competitive landscape of high-frequency arbitrage.

## VI. Conclusion

### A. Main Findings and Contributions

This Systematization of Knowledge (SoK) paper provides a comprehensive survey and classification of arbitrage and attack strategies in Decentralized Finance (DeFi). Our main findings are as follows:

- We present a unified taxonomy of DeFi arbitrage, covering cross-platform, triangular, flash loan, oracle-based, and emerging MEV-driven strategies, and analyze their mechanisms, quantitative impacts, and systemic risks.
- We systematically classify DeFi attacks into technical and economic categories, detailing common smart contract vulnerabilities, oracle manipulation, MEV extraction, and composability-induced cascading failures.
- Through comparative case studies and quantitative analysis, we reveal the dual role of arbitrage and attacks in both enhancing market efficiency and amplifying systemic risk.
- We review and evaluate state-of-the-art defense mechanisms, including formal verification, oracle enhancements, MEV mitigation, incentive-compatible mechanism design, and community governance frameworks.
- We identify key research gaps, such as cross-chain atomicity, scalable security solutions, and the need for interdisciplinary approaches integrating cryptography, economics, and regulatory science.

### B. Implications for DeFi Security and Ecosystem

Our analysis highlights that while DeFi unlocks unprecedented financial innovation and inclusiveness, it also introduces novel attack surfaces and amplifies systemic fragility due to composability and automation. The interplay between arbitrage and attack strategies challenges the clear boundaries of ethical and legal behavior, requiring adaptive governance and regulatory frameworks. Effective security in DeFi demands not only robust technical solutions but also incentive alignment, transparent governance, and continuous monitoring.

### C. Comparison with Related SoK and Foundational Works

Compared to prior SoK studies [1], [2], [4], our work offers a more granular taxonomy of arbitrage and attack strategies, incorporates the latest developments in MEV and cross-chain arbitrage, and emphasizes the gray area between legitimate arbitrage and malicious exploitation. We further bridge the gap between academic theory and real-world protocol incidents, providing actionable insights for both researchers and practitioners.

### D. Summary Table of Key Insights

TABLE II
SUMMARY OF KEY INSIGHTS FROM THIS SOK

| Aspect | Key Insight |
|---|---|
| Arbitrage Taxonomy | Multi-dimensional, evolving with MEV, cross-chain, and AI-driven paradigms |
| Attack Vectors | Technical (contract, oracle), economic (MEV, governance), composability risks |
| Defense Mechanisms | Multi-layered: formal verification, oracle design, MEV mitigation, incentive alignment |
| Governance | DAOs critical but face challenges in coordination, responsiveness, and capture |
| Open Challenges | Cross-chain security, scalable privacy, composability, interdisciplinary frameworks |
| Research Directions | Multi-agent simulation, knowledge graphs, quantum computing, climate impact |

### E. Final Remarks

DeFi represents a transformative shift in financial infrastructure, but its security and stability hinge on a holistic understanding of arbitrage and attack strategies. As the ecosystem continues to evolve, future research should prioritize cross-chain and composability risks, develop standardized security frameworks, and foster interdisciplinary collaboration. By integrating technical, economic, and governance innovations, the DeFi community can build a more resilient, fair, and sustainable decentralized financial system.

## REFERENCES


[1] S. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. Knottenbelt, "SoK: Decentralized finance (defi)," in *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies (AFT '21)*, 2021, pp. 1–15.

[2] J. Xu, B. Livshits, and A. Gervais, "Sok: Decentralized finance security and privacy," *arXiv preprint arXiv:2104.08739*, 2021. [Online]. Available: https://arxiv.org/abs/2104.08739

[3] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," https://ethereum.github.io/yellowpaper/paper.pdf, 2014.

[4] K. Qin, L. Zhou, and A. Gervais, "Quantifying blockchain extractable value: How dark is the forest?" in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 198–214.

[5] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, "Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 910–927.

[6] G. Angeris and T. Chitra, "Improved price oracles: Constant function market makers," in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (AFT)*. ACM, 2020, pp. 80–91.

[7] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 2016, pp. 270–282.

[8] J. Xu *et al.*, "SoK: Decentralized Finance (DeFi)," in *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, 2022. [Online]. Available: https://dl.acm.org/doi/10.1145/3558535.3559780

[9] K. Qin, C. Zhou, and A. Gervais, "Attacking the defi ecosystem with flash loans for fun and profit," *arXiv preprint arXiv:2003.03810*, 2021. [Online]. Available: https://arxiv.org/abs/2003.03810

[10] A. Shleifer and R. W. Vishny, "The limits of arbitrage," *The Journal of Finance*, vol. 52, no. 1, pp. 35–55, 1997.

[11] Y. Cao, C. Zou, and X. Cheng, "Flashot: A snapshot of flash loan attack on defi ecosystem," 2021. [Online]. Available: https://arxiv.org/abs/2102.00626

[12] M. Bichuch and Z. Feinstein, "Defi arbitrage in hedged liquidity tokens," 2024. [Online]. Available: https://arxiv.org/abs/2409.11339

[13] L. Zhou, K. Qin, A. Cully, B. Livshits, and A. Gervais, "On the just-in-time discovery of profit-generating transactions in defi protocols," 2021. [Online]. Available: https://arxiv.org/abs/2103.02228

[14] D. Wang, S. Wu, Z. Lin, L. Wu, X. Yuan, Y. Zhou, H. Wang, and K. Ren, "Towards a first step to understand flash loan and its applications in defi ecosystem," ser. SBC '21. New York, NY, USA: Association for Computing Machinery, 2021. [Online]. Available: https://doi.org/10.1145/3457977.3460301

[15] X. Deng, S. M. Beillahi, C. Minwalla, H. Du, A. Veneris, and F. Long, "Safeguarding defi smart contracts against oracle deviations," ser. ICSE '24. New York, NY, USA: Association for Computing Machinery, 2024. [Online]. Available: https://doi.org/10.1145/3597503.3639225

[16] J. Chen, X. Xia, D. Lo, J. Grundy, X. Luo, and T. Chen, "Defining smart contract defects on ethereum," *IEEE Transactions on Software Engineering*, vol. 48, no. 1, pp. 327–345, 2022.

[17] X. Wu, J. Xing, and X. Li, "Exploring vulnerabilities and concerns in solana smart contracts," *arXiv preprint arXiv:2504.07419*, 2025.

[18] P. Ince, J. Yu, J. K. Liu, and X. Du, "Generative large language model usage in smart contract vulnerability detection," *arXiv preprint arXiv:2504.04685*, 2025.

[19] A. T. Aspembitova and M. A. Bentley, "Oracles in decentralized finance: Attack costs, profits and mitigation measures," *Entropy*, vol. 25, no. 1, 2023.

[20] J. Cole, "Understanding dai smart contract audits: Security, governance, and implications," *BlockApps*, 2024.

[21] Z. Chen, S. M. Beillahi, P. Barahimi, C. Minwalla, H. Du, A. Veneris, and F. Long, "Secure smart contract with control flow integrity," *arXiv preprint arXiv:2504.05509*, 2025.

[22] L. Heimbach and R. Wattenhofer, "Eliminating sandwich attacks with the help of game theory," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, 2022, pp. 153–167.

[23] F. Salzano, L. Marchesi, C. K. Antenucci, S. Scalabrino, R. Tonelli, R. Oliveto, and R. Pareschi, "Bridging the gap: A comparative study of academic and developer approaches to smart contract vulnerabilities," *arXiv preprint arXiv:2504.12443*, 2025.