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].

Oracles: Oracles provide reliable access to off-chain data, which is critical for the correct functioning of DeFi applications. Oracles securely deliver external information, such as asset prices and event outcomes, to smart contracts on the blockchain [1].

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:

2) Representative Case Studies:

3) Quantitative Analysis of Profitability and Risks:

C. Triangular Arbitrage: Principles and Real-World Implementations

1) Arbitrage Path Construction:

2) Case Analysis: Successful and Failed Triangular Arbitrages:

3) Market Efficiency and Impact:

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

1) Flash Loan Fundamentals and Protocols:

2) Classic Flash Loan Arbitrage Cases:

3) Risk Factors and Systemic Implications:

E. Oracle-Based Arbitrage and Manipulation

1) Oracle Mechanisms in DeFi:

2) Arbitrage Strategies Leveraging Oracle Delays or Manipulation:

3) Case Studies and Defensive Measures:

F. Emerging Arbitrage Innovations

1) Novel Strategies (e.g., Multi-chain, Cross-layer, MEV-based):

2) Theoretical and Practical Challenges:

G. Comparative Case Studies and Quantitative Impact Analysis

1) Cross-Strategy Comparison Table:

2) Statistical Overview of Major Arbitrage Events:

3) Impact on DeFi Ecosystem Stability:

H. Summary and Research Gaps

III. Systematization of Attack Strategies

A. Taxonomy and Attack Models

1) Definition and Classification of Attacks in DeFi:

2) Attack Surfaces and Threat Models:

B. Smart Contract Vulnerability Exploits

1) Common Vulnerabilities (Reentrancy, Overflow, Logic Bugs, etc.):

2) Representative Exploit Cases:

3) Quantitative Loss and Post-Mortem Analyses:

C. Economic and MEV-Related Attacks

1) Flash Loan Attacks: Beyond Arbitrage:

2) Sandwich Attacks and Front-running:

3) MEV Extraction Techniques and Their Impacts:

4) Case Studies and Statistical Losses:

D. Oracle Manipulation Attacks

1) Manipulation Techniques:

2) Notable Cases and Consequences:

3) Theoretical Limits of Oracle Security:

E. Notable Cases, Loss Analysis, and Lessons Learned

1) Top Attack Incidents: Timeline and Loss Ranking:

2) Lessons for Protocol Designers:

F. Summary and Open Challenges

IV. Defense Mechanisms and Governance

A. Technical Defenses

1) Smart Contract Audits and Formal Verification:

2) Oracle Security Enhancements:

3) MEV Mitigation Techniques:

4) Case Studies: Defense Successes and Failures:

B. Economic Incentives and Mechanism Design

1) Incentive-Compatible Security Models:

2) Game-Theoretic Approaches:

3) Case Analysis: Effective Economic Defenses:

C. Community Governance and Incident Response

1) DAO-based Governance Mechanisms:

2) Incident Response and Recovery Case Studies:

3) Challenges in Decentralized Coordination:

D. Limitations and Challenges

1) Technical, Economic, and Social Limitations:

2) Open Problems:

E. Summary

V. Discussion and Future Directions

A. The Grey Area Between Arbitrage and Attack

1) Case Studies: Ethical and Legal Ambiguities:

2) Regulatory and Governance Implications:

B. Future Trends in the DeFi Ecosystem

1) Technological Innovations (e.g., AI, Layer 2, Cross-chain):

2) Regulatory Evolution and Global Trends:

C. Emerging Challenges for Research and Industry

1) Scalability, Privacy, and Composability:

2) Interdisciplinary Research Opportunities:

D. Open Research Directions

1) Key Open Questions:

2) Suggested Methodologies and Approaches:

VI. Conclusion

A. Main Findings and Contributions

B. Implications for DeFi Security and Ecosystem

C. Comparison with Related SoK and Foundational Works

D. Summary Table of Key Insights

E. Final Remarks

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.