

Decentralized Finance (DeFi) Platforms: Security and Scalability

Sakshi Malik

Jindal Global Business School, O.P. Jindal Global University, Sonapat, Haryana, India

M. Harish

Department of Business Administration, Faculty of Management, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India

M.R. Mathivanan

Department of IT, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamil Nadu, India

ABSTRACT: Decentralized Finance (DeFi) is a revolutionary breakthrough that is reconditioning the conventional finance space by leveraging transparent, permissionless, and blockchain-enabled services. The emerging blockchains are growing at a high pace in the past couple of years, revealing imperative security and scalability challenges that may impede their growth and widespread. Our work investigates the security vulnerabilities of DeFi protocols, covering smart contract attacks, oracle attacks, governance attacks, as well as the scalability bottlenecks of network saturation and increasing gas price. We present an extensive review of existing research literature from 2021 to 2025 in order to verify the practicality of the proposed systems, to answer the question whether existing solutions such as layer-2 scaling solutions, cross-chain interaction, and formal verification mechanisms can be practical. The paper also examines the trade-off between decentralization and performance, and points out what it takes to design DeFi ecosystems to be resilient and scalable, providing a roadmap to drive future research. The results will also help to advance the knowledge on how to protect decentralized infrastructure while maintaining high throughput and global reachability.

Keywords: DeFi security, blockchain scalability, smart contract risks, decentralized finance governance, interoperability solutions

73.1 INTRODUCTION

Decentralized Finance (DeFi) is a global financial platform that offers transparent, efficient, and open financial services through blockchain and crypto. However, its rapid development has led to security issues and poor scalability, threatening its stability and widespread application. Issues such as high transaction costs and slow transactions per second (TPS) on top blockchain infrastructures hinder DeFi's stability. To address these challenges, cost-effective solutions are needed to support secure operations at scale. The ultimate goal is to build long-lasting, robust, scalable, and secure DeFi infrastructure.

73.2 PROBLEM STATEMENT

DeFi (Decentralized Finance) projects are on the rise when it comes to redefining the dynamics of traditional finance, but have a number of drawbacks that affect its trust, scaling potential, and open reception. Open source smart contracts, decentralized governance being the default is in fact the biggest attack vector for a DeFi platform making it the least secure for hacks, protocol mismanagement (flashloans etc.) and systemic risks. Meanwhile, the DeFi solutions are proving ineffective in scaling up largely because they are built on technologies that put the entire ecosystem's transaction processing capability and overall performance under pressure, which results in long transaction time, high fees, and network rejections during peaks. Despite multiple projects emerging none have really coalesced around some coherent strategies that incorporate both the security and scaling aspects of DeFi. Without systemic solutions to these issues, they run a risk of stalling the metamorphosis of DeFi from an interesting niche to foundational financial infrastructure. This paper attempts to investigate and propose solutions for these urgent issues without violating the essential spirit of the decentralized ecosystem.

73.3 LITERATURE SURVEY

The evolving landscape of Decentralized Finance (DeFi) has attracted substantial academic attention, particularly concerning its security and scalability. Micheal (2025) highlights critical vulnerabilities in DeFi protocols and emphasizes the need for proactive risk mitigation. Capponi et al. (2023) explore governance and operational risks across various DeFi layers. Chaliasos et al. (2023) examine the limitations of existing security tools and the gap between theoretical development and real-world application. Ma et al. (2023) delve into governance inefficiencies, while Xiong et al. (2023) investigate market misconduct and policy implications. Schar (2022) and IOSCO (2022) provide foundational insights into regulatory and compliance challenges. Alon and Levy (2025) analyze DeFi’s systemic structure, and Abdulhakeem and Hu (2021) emphasize its role in financial inclusion.

73.4 METHODOLOGY

Method This paper takes a qualitative research approach based on systematic review of scientific articles, technical whitepapers and industry reports between 2021-2025. The research process includes seeking, evaluating, and compiling literature on security threats and scalability bottlenecks in DeFi platforms. We theme the findings to major focus areas, such as smart contract security, consensus methods, transaction throughput and cross-blockchain interoperability. To this end, we further complement the analysis of lighting network implementations (both in terms of static code analysis and runtime behavior) with case studies of both notorious DeFi exploits and scaling solutions in order to derive practical observations and achieve performance results. This approach facilitates a deep understanding of current solutions and their practical implications. A comparison between centralized and decentralized risk management and scalability is focused, by looking to the trade-offs between decentralization, efficiency and control. The approach contributes towards the construction of a conceptual framework that aims to improve the security and scalability of defi systems. Figure 73.1 and Table 73.1 shows the overview and scalability solution of DeFi platform focus areas.

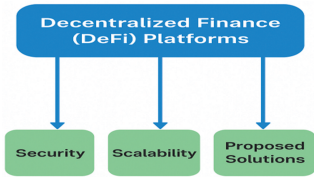


Figure 73.1. Overview of DeFi platform focus areas.

73.5 RESULTS AND DISCUSSION

The study reveals that DeFi applications, while offering a viable alternative to traditional financial services, still face security weaknesses and scalability issues. Reentrancy and logic flows contribute to financial loss, necessitating formal verification and automated auditing tools. Layer-2 solutions like rollups and sidechains offer effi-

Table 73.1. Scalability solutions in DeFi platforms.

Solution Type	Technology Examples	Benefits	Limitations
Layer-2 Scaling	Optimistic Rollups, zkRollups	Lower fees, higher throughput	Increased complexity, exit delays
Sharding	Ethereum 2.0	Parallel processing	Cross-shard communication issues
Sidechains	Polygon, xDai	Application-specific customization	Security reliant on sidechain model
Off-chain Computing	Chainlink OCR, zkApps	Reduces on-chain load	Trust assumptions, limited use

ciency but lower decentralization and new challenges for users. Governance is varied, and platforms struggle to balance community involvement with decision-making. Interoperability is being developed, but without standardized protocols, cross-chain communications risk arises. A hybrid model of on- and off-chain drivers is suggested for building resilient DeFi environments. The Table 73.2 shows Summary of Security Challenges in DeFi Platforms.

Table 73.2. Summary of Security Challenges in DeFi Platforms.

Security Layer	Common Threats	Example Incidents	Mitigation Techniques
Smart Contracts	Reentrancy, integer overflow	The DAO Hack (2016)	Formal verification, audits
Oracles	Price manipulation	bZx Attack (2020)	Decentralized oracles, aggregation
Governance	Voting manipulation	Compound Proposal Bug (2021)	Timelocks, delegated voting
Front-end	Phishing, DNS hijacking	BadgerDAO Frontend Hack (2021)	2FA, secure DNS, hardware wallets

73.6 CONCLUSION

Decentralized Finance (DeFi) has proven to have great potential to transform the state of finances, but still faces obstacles of security and scalability. The vulnerabilities of smart contracts and the governance models, as well as the performance of blockchain infrastructure they are relying on are the subjects of study in this research work. While emerging technologies like Layer-2 scaling and formal verification provide partial solutions, a combined, comprehensive treatment is necessary for the long-run success of the project. Secure and scalable DeFi systems call for ongoing innovation, inter-operating standards, and balancing of decentralization and efficiency. Developing these parts is important to DeFi's progression into a mainstream financial infrastructure.

REFERENCES

- [1] Micheal, L. (2025). *Evaluating the security challenges and risk mitigation strategies in decentralized finance protocols*. Retrieved from https://www.researchgate.net/publication/391279433_Evaluating_the_Security_Challenges_and_Risk_Mitigation_Strategies_in_Decentralized_Finance_ProtocolsResearchGate
- [2] Capponi, A., Iyengar, G., & Sethuraman, J. (2023). *Decentralized finance: Protocols, risks, and governance*. arXiv. <https://arxiv.org/abs/2312.01018>SSRN±2arXiv±2arXiv±2
- [3] Chaliasos, S., Charalambous, M. A., Zhou, L., Galanopoulou, R., Gervais, A., Mitropoulos, D., & Livshits, B. (2023). *Smart contract and DeFi security tools: Do they meet the needs of practitioners?* arXiv. <https://arxiv.org/abs/2304.02981>arXiv
- [4] Ma, W., Zhu, C., Liu, Y., Xie, X., & Li, Y. (2023). *A comprehensive study of governance issues in decentralized finance applications*. arXiv. <https://arxiv.org/abs/2311.01433>arXiv
- [5] Xiong, X., Wang, Z., Cui, T., Knottenbelt, W., & Huth, M. (2023). *Market misconduct in decentralized finance (DeFi): Analysis, regulatory challenges and policy implications*. arXiv. <https://arxiv.org/abs/2311.17715>arXiv