GJETA

Global Journal of Engineering and Technology Advances

eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

Global Journal of Engineering and Technology Advances
GJETA
eISSN:2582-5003
Global Scholar Press, INDIA

(Review Article)

Check for updates

Smart contract vulnerability in DeFi: Assessing security risk in blockchain-based lending platforms

Nonso Okika [1], Omoshalewa Anike Adeosun [2, *], Oluwatobi Julius Ogunjide [3] Blessing Unwana Umoh [4] and Modupe Elizabeth Temidayo [5]

[1] *Network Security Analyst, University of Michigan, U.S.A.*
[2] *Applied Cybersecurity, University of South Wales, Newport, United Kingdom.*
[3] *Independent Researcher, OTTA Global Venture, Nigeria.*
[4] *Department of Business Administration & Management of Information System, University of Pittsburgh U.SA*
[5] *Department of Management Information System, Bowie State University*

Global Journal of Engineering and Technology Advances, 2025, 22(03), 192-201

Publication history: Received on 31 January 2025; revised on 16 March 2025; accepted on 19 March 2025

Article DOI: https://doi.org/10.30574/gjeta.2025.22.3.0064

Abstract

The blockchain based smart contracts allow the creation of peer-to-peer lending in a decentralized finance model called DeFi. While Aave, Compound, and MakerDAO make it easier to gain access to capital and do away with middlemen, security breaches are highly likely to occur. This study analyzes the smart contract vulnerabilities such as reentrancy attacks, oracle manipulation, flash loan exploits, are systematically highlighted and their impact on projects in the market. Furthermore, it completes assessment beyond the security focus of liquidity volatility, regulatory uncertainty and fragmented risk management framework. A systematic literature review was adopted in the study with peer reviewed journal, industry report as well as case studies of past DeFi exploits. The key vulnerabilities, risk assessment methods, and mitigation frameworks are dealt as a theme. According to findings, although smart contract security has improved, DeFi is still very prone to exploitation for the lack of centralized oversight and standardised security measures. The study also brings our attention to the fact that risks in smart contract need continuous smart contract audits, formal verification schemes, and decentralized insurance mechanisms as well as regulatory collaboration. For the sustainable growth of DeFi lending platforms, such a balance should be made possible between technological security measures and improved governance and regulatory frameworks. The increased security mechanisms will increase the user trust and make decentralized lending an alternative to traditional financial systems.

Keywords: Decentralized Finance (DeFi); Smart Contract Vulnerabilities; DeFi Lending Security; Blockchain-Based Lending; Risk Mitigation in DeFi

1. Introduction

Decentralized Finance (DeFi) is transforming the financial sector by offering open, permissionless, and transparent architecture that handles financial services through the decentralized finance (DeFi) model [1]. Decentralized lending is a great innovation within DeFi, where users are able to lend and borrow assets without traditional financial intermediaries [2]. Unlike traditional banking, DeFi lending relies on smart contracts which automate loan dealing and remove intermediation institutions [3].

DeFi lending has been instrumental in the process of financial decentralization due to its ability to improve access to financial services, in particular, for unbanked and underbanked populations [4]. This means that the traditional banking institutions often impose stringent credit requirements, which lead to the exclusion of many individuals from getting

[*] Corresponding author: Omoshalewa Anike Adeosun Orcid: https://orcid.org/0009-0003-8249-009X

loans; however, DeFi enables anybody with internet access to participate in lending and borrowing activities [5]. Liquidity and security is ensured through the use of blockchain based collateralization mechanisms in the case of the most prominent DeFi lending platforms such as Aave, Compound and MakerDAO [6].

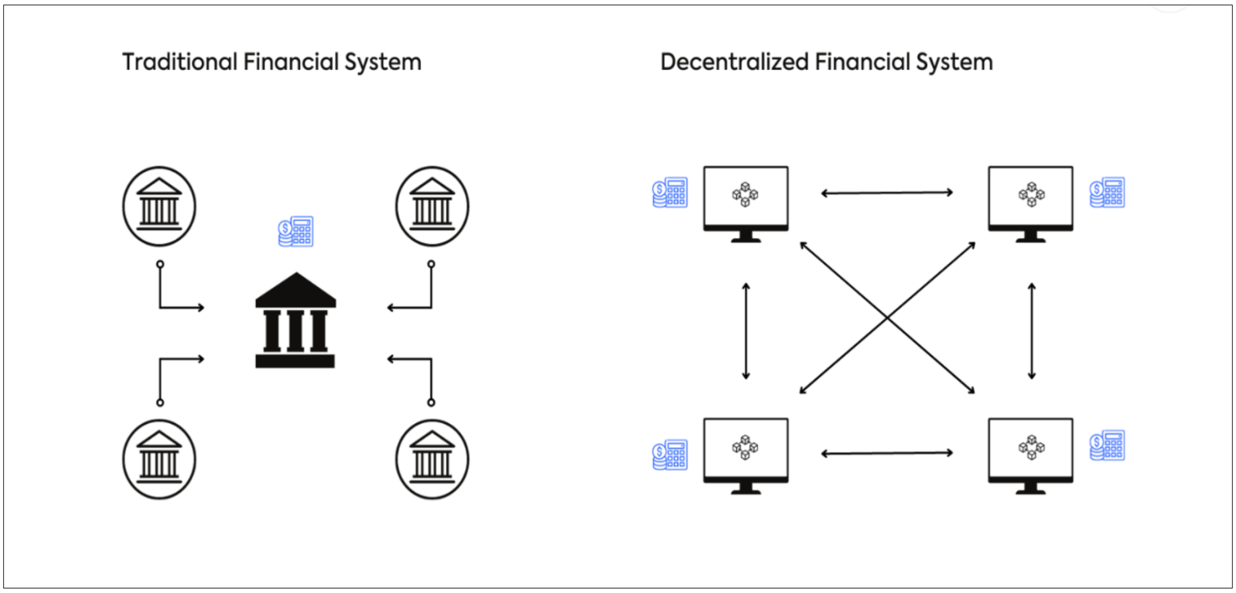

Figure 1 Traditional and decentralized financial system [7])

It leverages blockchain technology for the DeFi lending by making sure of the transparency and security through its immutable ledger that records all the transactions publicly [8]. But DeFi strips out intermediaries but also brings it with risk. As the DeFi lending lacks of regulatory oversight it is susceptible to security problems like smart contract vulnerabilities, cyberattacks, or manipulation of the market [9]. While DeFi lending is faster and cheaper than the traditional financial lending, it is also more prone to security breaches [3, 2].

DeFi lending is spearheaded by smart contracts which automate the key processes of issuance of loan, accrual of interest and liquidation of collateral [1]. The main benefits of blockchain include transparency, as all transactions are recorded publicly and thus there are lower risks of fraud [8]. They also facilitate decentralization due to the fact that users can control their assets without the dependence on financial institutions [4], improve efficiency by executing transactions automatically [3], and reduce transaction costs by doing away with third party fees [9]. In fact, though, there are limitations with smart contracts. They can be exploited so as to lead to financial losses [2]. Furthermore, there is a lack of centralized oversight to control fraud risks [1] and DeFi platforms are the common target of cyberattacks because users lock high value assets on them [5].

However, security is still a big problem with DeFi lending. This is because, with time, the attacks such as reentrancy exploits, oracle manipulation, and flash loan exploits have significantly led to financial losses [2]. DeFi operates outside of traditional finance, which employs regulatory measures to mitigate risks, and therefore DeFi platforms are at risk of being hacked and failing smart contracts [6]. Ensuring smart contract security while preserving decentralization is one of the biggest challenges. However, external audits and peer reviews used by DeFi platforms have usually failed to sufficiently catch security breaches [9,4]. These issues need to be addressed to make DeFi lending sustainable and secure for the long term [3]. For this reason, this research aimed to explore ‘Smart Contract Vulnerability in DeFi: Evaluating Security Risks on Blockchain-based Lending Platforms.’

1.1. Research Objectives

This study aims to:

- Identify common security vulnerabilities in DeFi lending smart contracts.
- Analyze real-world security breaches in blockchain-based lending platforms.
- Propose mitigation strategies for strengthening DeFi lending security.

1.2. Research Questions

- What are the most common smart contract vulnerabilities affecting DeFi lending platforms?
- How have past security incidents impacted DeFi lending ecosystems?
- What risk mitigation strategies can enhance DeFi lending security?

1.3. Significance of the Study

This research contributes to DeFi security literature by identifying vulnerabilities in lending protocols. This will help developers, auditors, regulators and users to understand how to improve security measures. This will allow developers to design more secure smart contracts, and auditors to identify risks, and regulatory discussions on the security of DeFi. To strengthen DeFi lending security and achieve trust, stability, and long-term adoption of blockchain based financial service is crucial.

2. Literature Review

2.1. The Role of Smart Contracts in DeFi Lending

DeFi lending platforms are based on smart contracts, which automate the transaction and enforce lending agreements without any intermediaries [10]. These contracts determine loan terms, collateral requirements and interest rates for users that want to lend and borrow assets without the necessity of a centralized intermediary. Smart contracts play a crucial role in leading DeFi lending protocols, such as Aave, Compound, and MakerDAO, by enabling overcollateralized loans, where borrowers must submit assets exceeding the loan value to reduce default risk.[11]. Smart contracts also make it possible to automate regulatory reporting, which improves compliance by lowering the need for human oversight and minimising mistakes. This increases the overall effectiveness of AML procedures, which results in quicker and more accurate fraud reporting and detection [12]. DeFi, at the same time, reduces operational costs and increases transaction speed due to the absence of traditional banking intermediaries. Despite these benefits, smart contracts introduce several limitations. One major concern is immutability, meaning that once deployed, smart contracts cannot be easily modified. While immutability enhances transparency, it also means that any coding flaws or logic errors remain embedded in the contract unless an upgrade mechanism is implemented [13]. This rigidity has led to multiple security breaches which can be exploited by attackers as they attack vulnerabilities that cannot be patched without modification to the protocol.

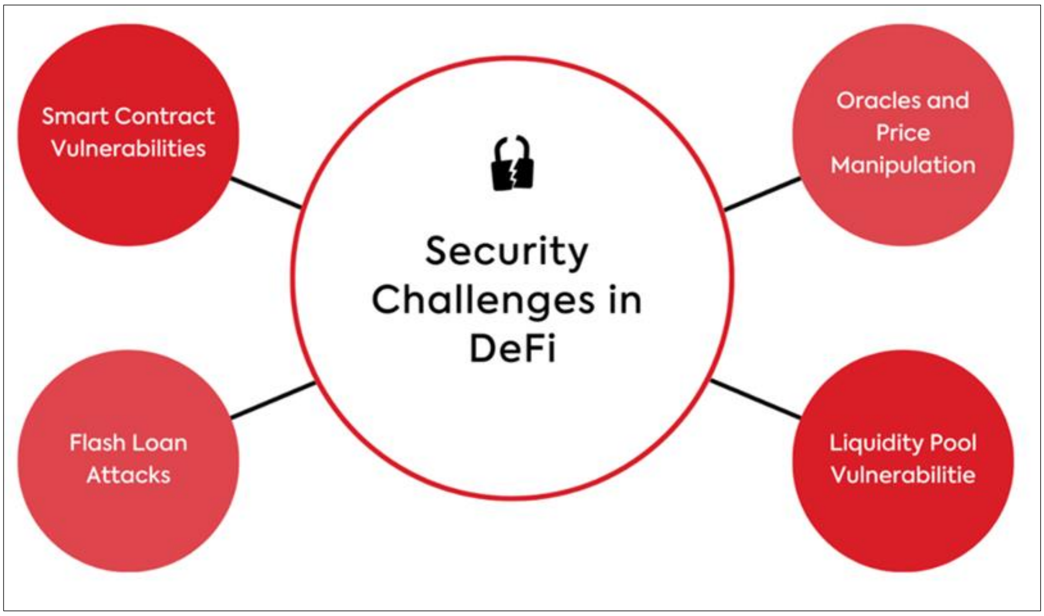
Smart Contract Vulnerabilities
Oracles and Price Manipulation
Security Challenges in DeFi
Flash Loan Attacks
Liquidity Pool Vulnerabilitie

Figure 2 Security challenges in DeFi; [7])

The second challenge is the reliance on price oracles that provide real time asset prices to DeFi lending contracts [14]. The price data that these oracles get is external and, if tampered, can lead to unexpected liquidations or price arbitrage attacks. For example, a sudden decrease in oracle reported price might cause a lender to believe that the borrower's collateral is below the minimum threshold, resulting in forced liquidation and monetary loss [15]. Smart contract operations also rely on the governance mechanisms. Decentralized Autonomous Organizations (DAOs) are quite common in many DeFi protocols; governance decisions, such as contract upgrades as well as risk management policies, are voted on by token holders [16]. Yet DAOs can be vulnerable to governance attacks where these malicious actors purchase enough of the DAO tokens to obtain a majority as their stake. Security threats due to governance-based attacks include the ability for attackers to change collateralization requirements or drain protocol funds [17].

2.2. Common Vulnerabilities in DeFi Lending Protocols

Multiple vulnerabilities in smart contracts on DeFi lending platforms have made them the target of various attacks. The vulnerabilities that these suffer from include reentrancy attacks, flash loan exploits, oracle manipulation, logic errors and governance attacks [14]. It is necessary to know these risks to develop appropriate security measures. Reentrancy is one of the most notorious smart contract vulnerabilities which is exploited by the attacker on how the contracts do external calls. Reentrancy attack occurs when a contract repeatedly calls itself without changing its internal state allowing an attacker to withdraw more money than they should [13]. Of course, the most infamous case is the 2016 DAO hack, which involved a reentrancy attack, draining around $60 million of Ether, and was followed by the poorly known controversy around a hard fork on Ethereum [18]. Since then, reentrancy guards have been implemented so that such attacks cannot occur. Developers follow Checks-Effects-Interaction's pattern in order to avoid recursive exploits and instruct state changes to take place before external calls [15].

A feature of flash loans is that users can borrow a lot of money without collateral with the stipulation that they have to repay the loan in a single transaction [14]. Flash loans were designed for arbitrage and liquidity provision; however, attackers have widely exploited it. In the bZx exploit the flash loans were used to artificially manipulate asset prices and suck liquidity out of the platform causing multimillion losses [16]. Oracles also have a very important role to play in DeFi lending, as they provide real time price data. Attackers try to manipulate low liquidity trading pairs as an oracle to create artificial price spikes or crashes, which will affect loan liquidations [10]. The Mango Markets exploit showed that the risk, as an attacker artificially inflated the price of the MNGO token, using overpriced asset as collateral to borrow large amounts of money before the price corrected, lost over $100 million [14]. Further security risks are compounded by governance attacks. In 2022, the Beanstalk governance exploit saw an attacker use a flash loan to buy voting power so as to pass a malicious proposal representing a steal of $182 million from the protocol [13]. To prevent such attacks [16], mitigation measures were proposed through multi signature approvals, time locked governance proposals, quadratic voting.

2.3. Security Incidents and Risk Mitigation Strategies

Based on DeFi security breaches frequency, it is clear that there is an urgent need for strong security measures in DeFi. Smart contract vulnerabilities financially and reputationally damage [18] such case studies as The DAO hack, bZx exploit and Cream finance. Several security measures have been adopted by DeFi platforms in response. Other leading security firms like CertiK, OpenZeppelin, or Even Trail of Bits audit smart contract before deployment [14]. While audits can evaluate at least some vulnerabilities, some only become evident under certain conditions [10].

As an increasing number of people rely on the security in contracts, formal verification which mathematically proves the contract correctness is used [15]. In addition, Bug bounty programs, for instance those hosted on Immunefi, encourage ethical hackers to identify vulnerabilities before they are exploited [17]. Decentralized insurance protocols such as Nexus Mutual and Cover Protocol also provide Dallas expanded insurance for DeFi exploits, financial protection to the users [18]. But vested interests according to [13] can manipulate governance votes to determine how much insurance payouts will be.

2.4. Theoretical framework

Davis (1989) [19] introduced the Technological acceptance model (TAM) for comprehension of user acceptance and trust of new technologies. It points at perceived usefulness (PU) and perceived ease of use (PEOU) as a major of adoption factors. TAM sheds light on why users participate in DeFi lending platforms when they exist in the context of security risks.

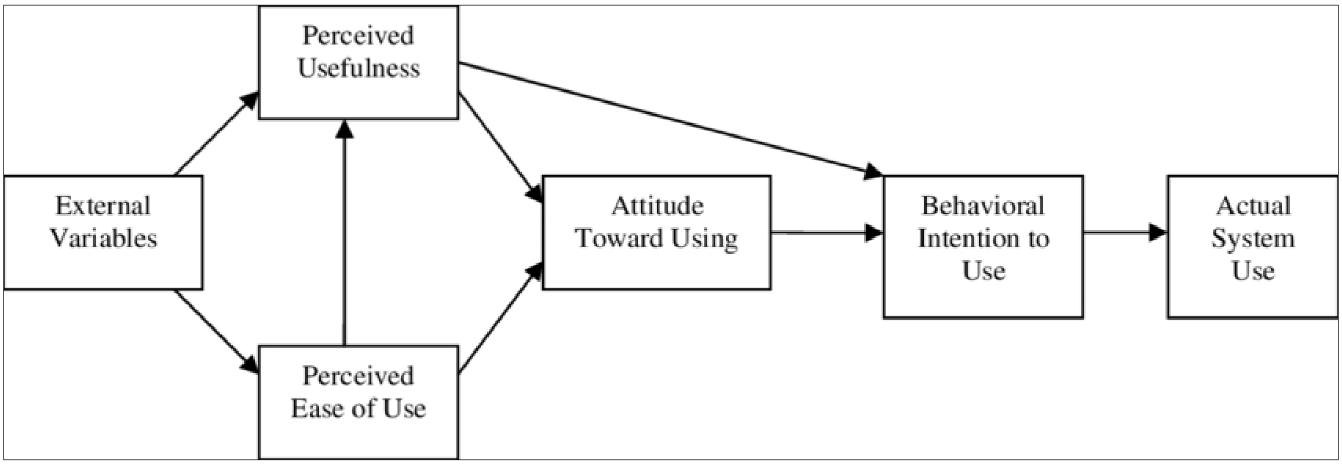

Figure 3 Technological acceptance model (TAM); [19]

DeFi is a proven approach to getting money in a new way, enjoying high yields, unlocked from geography and time, but these benefits depend on addressing very real security issues, such as smart contract weaknesses, governance attacks and oracle manipulation, which remain real barriers. For security purposes, shapers of user perception need to add smart contract audits and other security measures as trust is a vital attribute. Through Aave, Compound, and MakerDAO, de-finance lending platforms have changed the traditional financial systems by making it possible for users to lend and borrow without intermediaries [11]. Because of their permissionless nature and their algorithmic lending mechanisms, they provide great financial benefits, and thus are perceived as being useful. Nevertheless, numerous high-profile exploits have occurred that have resulted in financial losses via the DAO hack, bZx exploit, and Cream Finance attack [21]. Despite these risks, users continue to enter into DeFi for financial incentive and even overlook its security issue [22]. Another critical factor affecting adoption is the aspect of usability of the system. On account of many DeFi service provider platforms requiring technological background to interact with the smart contracts, manage the wallets, and pay the gas fees, they tend to be less available to non-technical user [10]. A poor PEOU has a negative impact on PEOU, which subsequently hampers adoption. In order to overcome this, DeFi protocols are enhancing user interfaces, automation, and educational resources to simplify interactions [17]. Formal verification also improves trust by mathematically proving, smart contracts are as they are intended to be, decreasing chances of exploits [15]. Between the benefits of financial benefit, usability and security, the application of TAM DeFi lending shows the importance of balancing. Perceived security matters tremendously to building trust where PU and PEOU drive adoption but security then becomes fatal. To sustain adoption and build long term confidence, DeFi platforms need to place strong security mechanisms on top of investing in a more seamless experience for users and risk management that is a canary hard for customer to catch what sunshine that they don't see and just what risk they are taking [16].

3. Research Methodology

This study adopts a Systematic Literature Review (SLR) methodology to critically examine the security vulnerabilities in DeFi lending platforms that are highlighted on the smart contract risks and the mitigation strategies. This approach of conducting the SLR facilitates identification, evaluation and synthesis of existing research in the blockchain based lending security challenges in a structured and transparent manner. With the rapid development of Decentralized Finance (DeFi) and its security status the SLR can serve as a good control method of know vulnerabilities, attack patterns and risk management practices. To incorporate the best of structured search strategy so that the data is collected comprehensively and unbiasedly. Literature sources associated with the study were sources from academic databases Google Scholar, IEEE Xplore, ScienceDirect, SpringerLink, industry white papers, security reports, blockchain audit firm publications. To narrow down the search, some keywords and Boolean operators (AND, OR, NOT) were used together. Key search terms included "DeFi lending security risks," "smart contract vulnerabilities in DeFi," "DeFi hacks and exploits," "blockchain-based lending security," "oracle manipulation in DeFi," "governance risks in decentralized lending platforms," "reentrancy attacks in smart contracts," and "risk mitigation strategies in DeFi." Citation chaining was also employed to identify influential studies referenced in key papers.

Inclusion and exclusion criteria were applied to make sure it was relevant. The studies were included if they explicitly examined security vulnerabilities in DeFi lending platforms, analyzed smart contract risks, governance attacks, or the mitigation strategies against exploit and provided the empirical evidence or detailed security analysis. To keep things focused, research in the areas of non-lending DeFi applications, general blockchain security or non-peer reviewed sources was excluded.

Data analysis was done through thematic categorization of security risks and its mitigation measures under structured themes. This review systemically classifies and analyzes these themes to provide a holistic view of security threat manifesting on DeFi lending platforms, and provide suggestions for platform to enhance their security framework endows with better auditing, verification and governance built.

4. Result and Discussion

4.1. Smart Contract Vulnerabilities in DeFi Lending Platforms

Just a few years ago, the world of finance was changing rapidly, and decentralized finance (DeFi) that utilizes blockchain technology and smart contracts amongst other things had begoten such a speed. Nevertheless, since smart contracts are involved, they possess high security risks for DeFi lending platforms [23]. It is particularly concerning that smart contracts execute financial transactions autonomously and without intermediaries, thus making it an ideal ground for exploitation. As shown in research work [24], billions of dollars in financial loses can happen due to the attacks on DeFi smart contracts, which makes the need for robust security mechanisms urgent.

There are different vulnerabilities in the smart contract, which can be divided into reentrancy attacks, oracle manipulation, logic error, and governance loopholes. Some of the largest DeFi exploits have been on account of reentrant attacks, where an attacker will repeatedly call a smart contract before the previous execution is completed [25]. In fact, DeFi lending platforms are also being exposed to another critical risk namely Oracle manipulation, where the price feed data is being filtered to execute trades at an artificially favorable rate [27]. At the same time, governance related vulnerabilities occur when malicious actors obtain control over decentralized autonomous organization (DAO) governance structures allowing them to change smart contract functionalities to make illicit gains [27]. While DeFi is experiencing an exponential growth, research suggests that there exists a gap of comprehensive security solutions capable of detecting and preventing the aforementioned vulnerabilities [24].

Several automated security tools are available, but they are not very effective, as the studies show that only a small fraction of past attacks could have been prevented by what exists in the detection mechanisms [25]. Faced with the lack of standardization in DeFi security, this becomes even worse since each protocol’s smart contract framework operates in an isolated fashion with dissimilar security measures [28].

The current rise in the DeFi adoption reflects the acute requirement for a higher level of smart contract auditing practices, constant threat detection and strong security frameworks. With DeFi growing its challenge of traditional financial systems, it is crucial to address these vulnerabilities to develop trust and make the decentralized financial ecosystem [29]. In the future, there will be need to collaborate between DeFi developers, security researchers and the regulator in order to mitigate risks and protect the security of smart contract based financial transactions. Had it not been for these developments, DeFi lending platforms will continue to be susceptible to more and more insightful cyber-attacks that threaten their sustainability[30].

Security concerns rise as the complexity of DeFi lending platforms increases and there’s a rise in number of new platforms offering more sophisticated functionalities without proper testing. As the industry introduces more technologies in the form of cross chain interoperability and layer 2 scaling solutions, these platforms become even more vulnerable to exploits [31]. Regardless of their strategy, DeFi validators and markets are being attacked that cleaves the delicate balance between economic security and security of the program [32]. Additionally, DeFi lacks consumer protection frameworks that could protect investors from unrecoverable financial loss as is the case in traditional finance, where institutions compensate investors in the event of fraud or technical error [23]. However, to address these risks, not only the security infrastructure of DeFi needs to be improved, but also the regulatory guidance should provide proper transparency and accountability while not abolishing the core principle of decentralization of DeFi [30]. As we move forward, real time security monitoring, AI based anomaly detection and decentralized insurance will be integral in making DeFi lending platforms resilient against the emerging threats and the ones that will continue to make it sustained and adopted [29].

4.2. Risk Assessment and Security Challenges

The rapid growth of DeFi brought security challenges that have never been encountered before, most notably, risk assessment and financial stability. Unlike traditional finance, DeFi operates in large part without crystallized regulatory framework and risks are inherently difficult to manage [23]. Since there is no centralized oversight of DeFi protocols, they need to have internal security mechanisms that frequently fail to address new threats [28]. It's important to bear in mind as DeFi explodes, that there's a special risk landscape to it and that's need for protecting investors and protecting the resiliency of decentralized systems. At the security element, a large number of smart contract bugs and vulnerabilities are one of the major security concerns in DeFi. The fact that DeFi platforms have been losing billions of dollars through flaws in the coding of their smart contract is the justification for the need of robust detection and mitigation strategies of vulnerabilities [23]. Automated security tools have been developed to detect vulnerabilities, but their effectiveness is limited [26] as studies show that they cannot prevent most of attacks. In addition, there is no standardized risk assessment framework that investors and developers can use to assess the security of DeFi protocols [27]. A liquidity volatility risk is another major risk in DeFi. Unlike the traditional financial institutions that have regulatory requirements to maintain liquidity, DeFi protocols use algorithmic mechanisms that can be highly subject to market fluctuations [26]. As a result of this volatility, DeFi lending markets have been greatly disrupted with mass liquidations and destabilizing of financial ecosystems [30]. Additionally, decentralised oracles are used by reliability for the lack of price feeds, but this brings further risk due to their manipulability for the creation of artificial market conditions [29]. On top of that, regulatory uncertainty is a major DeFi security problem. While there has been DeFi regulation in some jurisdictions, it varies from one jurisdiction to another, and has made compliance efforts more fragmented [33]. This poses high risks of illicit activities such as money laundering, fraud, and market manipulation in DeFi ecosystems [31]. To alleviate these worries, the regulators and industry pieces should work together to create a thorough risk management stage that balances financial reliability and innovation [32]. Without a structured risk assessment and security, DeFi will remain at a disadvantage when it comes to the mainstream adoption. To reduce risk and make DeFi ecosystem more resilient, strengthening security protocols, improving smart contract auditing practices, as well as regulatory clarity is essential [23].

Moreover, algorithmic liquidations in DeFi have come with unintended systemic risks, especially during market lows. Unlike traditional central financial institutions which are protected by liquidity buffers and regulatory safeguards, DeFi protocols usually have automated liquidation programs that do not only liquidate but can also multiply the liquidation by initiating forced liquidations (chain reactions) which makes itself worsen the financial instability [26]. On top of that, there is no industry-wide liquidity risk management framework that makes DeFi's long term viability even more complicated, and thus DeFi needs to integrate adaptive collateralization models and liquidity reserves to avoid huge market shocks [30]. For moving forward, developers, security firms, and regulators will need to work together to develop structured risk assessment protocols that would improve DeFi's resilience and facilitate the wider adoption of DeFi by institutions [23].

4.3. Mitigation Strategies and Security Frameworks

As DeFi expands there is great need for effective security frameworks and mitigation implements. Addressing the vulnerabilities inherent to DeFi lending platforms is a multifaceted problem both technologically, through solutions; and through legal frameworks and collaborative trust and security [23]. The main challenge being that DeFi's protocols are not built on practical strategies such as smart contract audits, decentralized insurance models, and robust governance profound strategies to further guarantee the security of DeFi protocols [28]. DeFi Security Smart contract audits are among the most widely used security measures in DeFi. Regular auditing by professional security companies to diagnose vulnerabilities before they can be exploited, and thus reduce the risk of such catastrophic financial losses [23]. But despite that, research has shown that simply audits are not enough, as many DeFi hacks exploit overlooked vulnerabilities that were not discovered in the initial security reviews [25]. As a result, auditing has to be complemented by ongoing monitoring and real time detection mechanisms for threats [29]. It is also linking to a decentralized insurance risk mitigating strategy. Decentralized insurance mechanisms [27], contribute to building the investor confidence in DeFi protocols by compensating the users when the exploit occurs through pooled funds. Despite these, these models remain in their infancy and are faced with challenges of deciding on a proper risk assessment and how to manage potential payout disputes [30].

In securing DeFi platforms, governance structures have an enhanced role. DAOs allow for decentralized governance which provides an opportunity for community driven decision making that has the ability to enhance the resilience of protocol against security threats [26]. However, governance vulnerabilities of DeFi protocols are still a concern for malicious actors to control voting mechanisms [33]. There are a number of ways in which these risks can be mitigated; they can be strengthened governance frameworks through better voting mechanisms and security focused upgrades [32]. In addition, DeFi needs regulatory clarity for the long-term security and sustainability of the same. Although DeFi is outside the traditional financial regulations, there are clear guidelines on the regulations of compliance, anti-money laundering (AML) protocols and investors protections that can make it legitimate [31]. This can be done with striking the balance between decentralization and regulatory oversight, thus providing more security and wider adoption [23].

Therefore, to tackle DeFi risks it is paramount to have an overall security framework which combines audits, decentralized insurance, upgrades in governance, and regulatory alignment. With this strategy, DeFi platforms can increase their resilience and keep the decentralized financial services long term sustainable.

Recommendations

DeFi lending platforms must adopt a multifaceted approach that includes technological, governance, and regulatory measures to enhance their security and long-term sustainability. The first thing is to make sure the smart contract security is ensured by rigorous and continuous auditing processes. In contrast to pre deployment audits DeFi protocols ought to have real time security monitoring and automated vulnerability detection mechanisms in order to detect and eliminate threats as they pop up. In addition, good coders can also follow secure coding practices as well as make use of formal verification techniques to reduce the probability of having exploitable vulnerabilities. Further development related to decentralized insurance should also be considered to protect users from financial losses caused by failure of smart contract or attacks. Some decentralized insurance models already exist but need to be improved with more robust risk assessment frameworks to ensure a fair and sustainable way of paying users who are affected by the decentralization. Such mechanisms should be integrated with smart contracts to pay automatically when security breaches occur. It also means, governance structures of DeFi lending platforms have to be strengthened to avoid centralization and manipulative exploits risk. To minimize governance attacks on the DAOs, multi signature authentication and improved voting mechanisms should be integrated into the decentralized autonomous organizations. One way to ensure the undue influence of a small group of actors does not lead governance decisions is by implementing minimum participation thresholds for governance decisions.

On a regulatory level, we need to take a balanced approach for security while maintaining DeFi’s untrusted nature. The regulatory frameworks should ensure the standardized security measures like identity verification for high-risk transaction should be implemented without hampering the permissionless and borderless nature of blockchain based finance. Regulators, with the help of their industry stakeholders and DeFi developers can help in the development of adaptive compliance mechanisms rooted to the changing landscape of decentralised finance. Moreover, user education and awareness programs should be promoted to educate decentralized lending users about the risks and security measures involved in DeFi. Smart contracts should be used by users to do a little bit of due diligence before interacting with the smart contract and to use multi factor authentication or cold storage solutions for protecting their assets. By increasing the literacy in blockchain security, a more resilient DeFi ecosystem will be achieved.

5. Conclusion

DeFi lending platform has brought about a revolution to the financial services with its decentralized, transparent, and permission less lending mechanism. However, their rapid expansion has shown to be very security risky, such as smart contract vulnerability, governance exploit, and regulatory uncertainty. DeFi’s frequency of cyberattacks and financial losses are the proof that the security needs of these projects are paramount to robust security frameworks and risk mitigation strategies. To tackle these challenges, security of the smart contract platform calls for a holistic security offering that takes the form of: continuous smart contract auditing, enhanced formalism associated with governance structures, and decentralized insurance modes. DeFi platforms can trim down on the risks of financial exploitation and operational failures by being proactive in the identification and mitigating vulnerabilities. Also, there must be regulatory clarity in place, which allows the DeFi ecosystem to stay in accordance with legal frames without undermining those principles that makes DeFi great, such as decentralization and financial inclusion.

In addition to the mentioned, governance improvements are key on solidifying the resilience of DeFi lending platforms as well. Transparent and tamper-proof voting mechanisms can prevent governance attacks against decentralized finance protocols. In addition, algorithmic risk assessment models can automate portfolio optimization, enhancing liquidity management, which would help to lessen the adverse effects of market volatility. Look, DeFi still has its challenges, but it is a force to reckon with in the global finance world; it not only offers innovative solutions but also extends financial access to the underserved. However, its future viability hinges upon the integration of proactive security protocols, regulatory alignment, and educational resources for the users. Overcoming security challenges is vital to ensuring DeFi is a safe space for all users; this will require working with regulators to develop frameworks that promote innovation while maintaining user safety and security. Trust and stability will be crucial to ensuring that DeFi lending platforms can serve as a true alternative to traditional financial systems.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Ali A. Decentralized finance (DeFi) and its impact on traditional banking systems: Opportunities, challenges, and future directions [Internet]. SSRN; 2024. Available from: https://ssrn.com/abstract=4942313 or http://dx.doi.org/10.2139/ssrn.4942313

[2] Bakare F, Omojola J, Iwuh A. Blockchain and decentralized finance (DeFi): Disrupting traditional banking and financial systems. World J Adv Res Rev. 2024;23(3):3075–89. https://doi.org/10.30574/wjarr.2024.23.3.2968

[3] Harvey CR, Rabetti D. International business and decentralized finance. J Int Bus Stud. 2024;55:840–63.

[4] Muhammad A, Ahmad Ishaq A, Mike M, Ibitomi T, Ishaq N, Isyaku M. Decentralized finance (DeFi) and traditional banking: A convergence or collision. Econ Polit Reg Dev. 2024;5(1):1. https://doi.org/10.22158/eprd.v5n1p1

[5] Abdulhakeem SA, Hu Q. Powered by blockchain technology, DeFi (decentralized finance) strives to increase financial inclusion of the unbanked by reshaping the world financial system. Mod Econ. 2021;12(1):1–X. https://doi.org/10.4236/me.2021.121001

[6] Ahmed A. The rise of DeFi: Transforming traditional finance with blockchain innovation [Internet]. 2024. Available from: https://doi.org/10.20944/preprints202402.0738.v1

[7] Chahal K. Security and safety of decentralized finance (DeFi) platforms [Internet]. WeSecureApp; 2024. Available from: https://wesecureapp.com/blog/security-and-safety-of-decentralized-finance-defi-platforms/

[8] Shah K, Lathiya D, Lukhi N, Parmar K, Sanghvi H. A systematic review of decentralized finance protocols. Int J Intell Netw. 2023;4:171–81.

[9] Grassi L, Lanfranchi D, Faes A, Renga FM. Do we still need financial intermediation? The case of decentralized finance – DeFi. Qual Res Account Manag. 2022;19(3).

[10] Schär F. Decentralized finance: On blockchain- and smart contract-based financial markets. Rev Fed Reserve Bank St Louis. 2021;103(2):153–74. https://doi.org/10.20955/r.103.153-74

[11] Kaplan B, Benli F, Alp E. Decentralized finance and new lending protocols. Pressacademia. 2023. https://doi.org/10.17261/Pressacademia.2023.1686

[12] Bello A A, Oduro D A, Manu E O, Bello A D, Leo A O, Ukatu C E, Okika N. Enhancing Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance using blockchain: A business analysis approach. Iconic Research and Engineering Journals. 2025;8(9):297-305.

[13] Mason J, Amelia O. Emerging threats and mitigation strategies in cyber security: A comprehensive guide for financial services and strategic management. ResearchGate. 2024. https://doi.org/10.13140/RG.2.2.25946.35525

[14] Li W, Bu J, Li X, Peng H, Niu Y, Zhang Y. A survey of DeFi security: Challenges and opportunities. J King Saud Univ Comput Inf Sci. 2022;34(10, Part B):10378–404.

[15] Adamyk B, Benson V, Adamyk O, Liashenko O. Risk management in DeFi: Analyses of the innovative tools and platforms for tracking DeFi transactions. J Risk Financ Manag. 2025;18(1):38. https://doi.org/10.3390/jrfm18010038

[16] Weingärtner T, Fasser F, Sá da Costa PR, Farkas W. Deciphering DeFi: A comprehensive analysis and visualization of risks in decentralized finance. J Risk Financ Manag. 2023;16(10):454. https://doi.org/10.3390/jrfm16100454

[17] Kaur S, Singh S, Gupta S, Wats S. Risk analysis in decentralized finance (DeFi): A fuzzy-AHP approach. Risk Manag. 2023;25:Article 13.

[18] John K, Kogan L, Saleh F. Smart contracts and decentralized finance. Annu Rev Financ Econ. 2023;15:523–42. https://doi.org/10.1146/annurev-financial-110921-022806

[19] Davis FD. A technology acceptance model for empirically testing new end-user information systems: Theory and results [Internet]. Massachusetts Institute of Technology; 1985. Available from: http://hdl.handle.net/1721.1/15192

[20] Miller J, Khera O. Digital library adoption and the technology acceptance model: A cross-country analysis. Electron J Inf Syst Dev Ctries. 2010;40:1–19. https://doi.org/10.1002/j.1681-4835.2010.tb00288.x

[21] Admass WS, Munaye YY, Diro AA. Cyber security: State of the art, challenges, and future directions. Cyber Secur Appl. 2024;2:100031.

[22] Li W, Bu J, Li X, Chen X. Security analysis of DeFi: Vulnerabilities, attacks, and advances. 2022 IEEE Int Conf Blockchain (Blockchain). 2022:488–93. https://doi.org/10.1109/Blockchain55522.2022.00075

[23] Ali A, Dembo SAS. Decentralized finance (DeFi) and its impact on traditional banking systems: Opportunities, challenges, and future directions. J Econ Res Rev. 2024;4(3):1–10.

[24] Qian P, Cao R, Liu Z, Li W, Li M, Zhang L, et al. Empirical review of smart contract and DeFi security: Vulnerability detection and automated repair. arXiv. 2023;abs/2309.02391. https://arxiv.org/abs/2309.02391

[25] Chaliasos S, Charalambous MA, Zhou L, Galanopoulou R, Gervais A, Mitropoulos D, et al. Smart contract and DeFi security tools: Do they meet the needs of practitioners? In: Proceedings of the 46th IEEE/ACM International Conference on Software Engineering (ICSE '24) [Internet]. 2024. Available from: https://doi.org/10.1145/3597503.3623302

[26] Alamsyah A, Kusuma GNW, Ramadhani DP. A review on decentralized finance ecosystems. Future Internet. 2024;16(3):76. https://doi.org/10.3390/fi16030076

[27] Melnikov I, Lebedeva I, Petrov A, Yanovich Y. DeFi risk assessment: MakerDAO loan portfolio case. Blockchain Res Appl. 2024. Advance online publication.

[28] Hinneh A. Risk management in decentralised finance (DeFi). Academia. 2024;72.

[29] Ahuja R, Khandelwal J, Anjali. Challenges, opportunities, and risk analysis of adoption of decentralized finance applications. Innov Technol FinTech (ITFT-2023). 2023;Special Issue:3114. https://doi.org/10.21917/ijsc.2023.0438

[30] Ikegwu C, Uzougbo N, Adewusi A. Regulatory frameworks for decentralized finance (DeFi): Challenges and opportunities. GSC Adv Res Rev. 2024;19:116–29. https://doi.org/10.30574/gscarr.2024.19.2.0170

[31] Benson V, Turksen U, Adamyk B. Dark side of decentralised finance: A call for enhanced AML regulation based on use cases of illicit activities. J Financ Regul Compliance. 2023;32(1).

[32] Mirdala R. Revolutionizing finance: Decentralized finance as a disruptive challenge to traditional finance. TPREF. 2024;15(3). https://doi.org/10.14505/tpref.v15.3(31).02

[33] Roy D, Dubey A, Tiwary D. Conceptualizing an institutional framework to mitigate crypto-assets' operational risk. J Risk Financ Manag. 2024;17(12):550. https://doi.org/10.3390/jrfm17120550