MUHASEBE VE FİNANS İNCELEMELERİ DERGİSİ
2018
MUFİDER

MUFİDER, 9, 1(2026), 42 – 54

CAUSES OF SECURITY VULNERABILITIES IN DeFi PLATFORMS AND PROPOSED SOLUTIONS

DeFi PLATFORMLARINDAKİ GÜVENLİK AÇIKLARININ NEDENLERİ VE ÇÖZÜM ÖNERİLERİ

Batuhan KARABAY [a*]

[a*] *Corresponding Author, Dr., Independent Researcher,* batuhan_karabay@hotmail.com, *ORCID: 0000-0002-5691-3947.*

ARTICLE INFO

Article history:
Received 28.09.2025
Revised 11.11.2025
Accepted 01.12.2025

Keywords: DeFi, security vulnerabilities, decentralized finance, Ethereum Layer-2, Zero-Knowledge, case study

Jel Codes: G23, G28, G32

RESEARCH ARTICLE

ABSTRACT

This study investigates the rising security vulnerabilities in decentralized finance (DeFi) platforms from both technical and operational perspectives. Through literature review, case studies, and a comparative platform analysis, the research identifies the root causes, user impacts, and mitigation strategies for common security issues. Prominent incidents such as Ronin Network, Poly Network, Mango Markets, and Curve Finance are examined in depth, while security strategies of major DeFi platforms such as Aave, Compound, Uniswap, and Synthetix are compared. The study also discusses the implications of new technological developments like Ethereum Layer-2 solutions, Zero-Knowledge rollups, and account abstraction mechanisms on DeFi security. Findings emphasize that achieving a sustainable DeFi ecosystem requires a holistic approach involving not only technical safeguards but also transparent governance, user education and robust audit processes.

MAKALE BİLGİLERİ

Makale Tarihçesi:
Gönderilme Tarihi 28.09.2025
Düzenleme 11.11.2025
Kabul Tarihi 01.12.2025

Anahtar Kelimeler: DeFi, güvenlik açıkları,

ÖZET

Bu çalışma, merkeziyetsiz finans (DeFi) platformlarında son yıllarda artış gösteren güvenlik açıklarını teknik ve operasyonel boyutlarıyla incelemektedir. Literatür taraması, vaka analizleri ve karşılaştırmalı platform değerlendirmesi yoluyla, bu açıkların nedenleri, kullanıcılar üzerindeki etkileri ve çözüm stratejileri kapsamlı şekilde ele alınmıştır. Ronin Network, Poly Network, Mango Markets ve Curve Finance gibi önemli vakalar üzerinden güvenlik sorunlarının yapısal boyutları ortaya konulmuş; Aave, Compound, Uniswap ve Synthetix gibi platformların uyguladığı güvenlik yaklaşımları karşılaştırılmıştır. Ayrıca,

APA STİLİ KAYNAK KULLANIMI: Karabay, B. (2026). CAUSES OF SECURITY VULNERABILITIES IN DeFi PLATFORMS AND PROPOSED SOLUTIONS. *Muhasebe ve Finans İncelemeleri Dergisi*, 9(1), 42 – 54. DOI: 10.32951/mufider.1792581

merkeziyetsiz finans, Ethereum Layer-2, Zero-Knowledge, vaka analizi
Jel Kodları: G23, G28, G32

ARAŞTIRMA MAKALESİ

BENZERLİK/ PLAGIARISM

Ithenticate: %9

Ethereum Layer-2 çözümleri, Zero-Knowledge rollup teknolojileri ve hesap soyutlaması gibi yeni gelişmelerin DeFi güvenliğine olan katkısı tartışılmıştır. Sonuç olarak, sürdürülebilir bir DeFi ekosistemi için teknik güvenliğin ötesinde yönetişim, kullanıcı eğitimi ve denetim süreçlerinin de bütüncül şekilde ele alınması gerektiği vurgulanmaktadır.

1. INTRODUCTION

DeFi has gained a lot of traction for being one of the most significant innovations to emerge in the recent evolution of fintech. It is this model that promises to erode our dependence on centralized intermediaries in traditional financial systems and which is quickly gaining popularity thanks to the transparency, reach and cost efficiencies offered by blockchain technology. From a Total Value Locked (TVL) of millions in 2018, DeFi advanced to hundreds of billions by 2021 and became the foundation for the creation of a global financial subsystem. This expansion has not only piqued the interest of retail and institutional players, which has been interpreted in some studies as a step toward financial democratization.

The most revolutionary aspect of DeFi is the combination of traditional banking services, such as credit and lending, exchange trading and specific derivative products and insurance in a decentralized and automated fashion using smart contracts. Users have the ability to make financial transactions similar to conventional banking transactions with this feature, significantly reducing transaction fees and removing geographical constraints. But a decentralized system has also created entirely new points of failure, such as lack of oversight, regulation and technical weakness. It is this paradox of "innovation and security" that defines DeFi today, becoming one of the most discussed issues that will structure what it becomes.

These very public incidents provide evidence of systemic vulnerabilities. For instance, in 2021 alone there was the Poly Network attack which resulted in more than $600 million worth of assets being stolen; the Ronin Network hack which cost around $625 million in 2022; and the Mango Markets exploit that caused $120 million of damage also last year; and a compiler-error-related vulnerability at Curve Finance in 2023 where hundreds of millions of dollars were put at risk. Examples such as these illustrate how vulnerabilities do not result solely from technical programming mistakes, but also from governance, end-user understanding and oversight shortfall. So, DeFi security is not a one-dimensional issue — it actually comprises technical, operational, and human aspects.

There are also economic and social consequences of DeFi security vulnerabilities that can't be ignored. On the one hand, the hard-earned savings of retail investors are at stake; on the other hand, loss of trust in the system results in rapid drawdowns in liquidity and greater market volatility. This lack of trust not only damages DeFi platforms, but also the wider crypto asset markets. Yet the unregulated nature of DeFi is fueling serious discussion in those successive jurisdictions about global regulation, including money laundering and terrorist financing. In this context, security is more than just a technical issue – it's a holistic problem involving financial health, regulation and user interests.

A lot of the existing literature regarding security in DeFi is concerned with technical weaknesses at the smart contract level. Reentrancy vulnerabilities, oracle manipulations, flash loan attacks and protocol structures of bridge etc. are often discussed. But there are also challenges, including the concentration of governance tokens, low participation rates and questions about the sustainability of community-run insurance systems. New technical innovations – like Ethereum Layer-2 solutions, zk-Rollup-based scalability models and computation abstraction standards (EIP-4337) were presented as promising answers to these problems, with new risks in return. Thus, the security of DeFi is a multi-faceted and ongoing research domain.

The overall goal of this research is to conduct a comprehensive investigation on security vulnerabilities

in DeFi applications (i.e., how and what the vulnerabilities are behind it and their implications, compare existing solutions, and provide some insights toward the future. The study seeks an integrated perspective to governance, user behaviour and regulation dimensions that have unfortunately been largely neglected in the literature. Thereby it also adds to the state of the art and offers an orientation framework for developers, investors, as well as policy makers.

Existing work focused predominately on technical risks in DeFi systems, however an integrated picture of relations between technical vulnerabilities as well as governance and user behaviour were less available. To the best of our knowledge, this limitation could be improved with the following research questions to be addressed in this research:

RQ1: What are the security vulnerabilities of DeFi projects from the technical, governance and user sides?

RQ2: What mechanisms (audit, insurance, governance transparency, technical control) that may mitigate these security vulnerabilities work most effectively?

RQ3: How do security architecture and policies differ between the top five DeFi platforms (Aave, Compound, Uniswap, Curve, Synthetix)?

This paper endeavours to investigate these research questions and contribute well-rounded multi-level insights into DeFi security beyond just the technology aspects, but also human and organization dimensions.

2. LITERATURE REVIEW

In light of the explosive expansion of the DeFi ecosystem, security problems for platforms have been focused on a wide range of research at an academic and industry level. Security vulnerabilities frequently found in literature are reentrancy attacks, oracle manipulation and flash-loan attacks, and maintenance-related issues and private-key security. The vast majority of these weaknesses result from lacking review of smart contract code or single points of failure in centralized architectures.

Qin et al. (2021), consider the idea of flash loans in DeFi space to show how such mechanism has two sides of the same coin, with its opportunities and risks. The paper demonstrates that both uncollateralized, and atomic transaction-based flash loans optimize arbitrage efficiency and liquidity usage at the same time; however they are vulnerable to attacks such as oracle manipulation, pumping prices, and manipulating the market. Some attacks have generated hundreds of thousands of dollars and were not even optimized with the current parameters so there is more potential. In addition, it is noted that flash-loan pools with billions in liquidity, as in platforms such as Aave, present systemic risks. In general, it can be concluded that flash loans stimulate financial innovation in DeFi but a thorough auditing and design approach is needed with regulator posture to mitigate the security issues presented by this literature.

In another study by Wang et al. (2021), security issues and attack vectors in decentralized finance (DeFi) are reviewed, and a threat detection system called BLOCKEYE is presented to detect them. The paper also highlights that user funds are under threat from attacks as a result of the open nature of DeFi projects, and introduces two main characteristics of BLOCKEYE: (i) leveraging symbolic analysis to discover oracle dependencies and potential attack vulnerabilities, and (ii) monitoring suspicious transactions through off-chain transaction logging. Applications on several Ethereum projects have demonstrated that the BLOCKEYE uncovers unreported attacks. The system can detect suspicious operations with high returns in a short time by modeling oracle dependence and analyzing transaction sequences end to end. The presented results demonstrate the need to account for economic dependencies and market interactions, opposing previous tools that solely focus on vulnerable smart contract mistakes in DeFi security analysis.

Li et al. (2022) systematically categorised DeFi security attack factors in a layered model from protocol / infrastructure and application / smart contract levels. They applied these vulnerabilities to real-world cases such as flash loan exploits and bridge attack, dissecting their technical and economic grounds. The article also surveyed the specific risk profile and attack model for popular DeFi components (e.g., DEXs, lending platforms, oracles, wallets etc.), as well as summarized and compared existing solutions for detection/thefts — such as static/dynamic analysis, formal verification, network/consensus level improvements. The paper concluded by

discussing operational considerations and presenting a list of potential future research avenues including automatic detection tools, secure delivery strategies oriented to efficiency.

In the work of Roșca et al. (2023), honing in on the scalability challenge of Ethereum, compare different Layer-2 solutions (optimistic rollups, zk-Rollups, state channels, plasma and sidechains) from the security standpoint; they stress that while zk-Rollups show very high TPS potential e.g., >2000 TPS, those carry separate risks because of design complexity and data availability. The post explains the specific attack vectors including delays resulting from fraud-proof periods in optimism rollups and invalid state roots, partial censorship risk as well as single point of failure threats presented by sequencer/operator centralization and "mass exit" weaknesses in plasma/sidechains. It also mentions issues with security/performance/quantum-resistance in ZK protocols (SNARK/STARK/PLONK), that Layer-2 designs should have data availability solutions, democratization of operators and strict upgrade management with formal verification.

In a research by Adarbah et al. (2024), a new secure, privacy-preserving and scalable architecture for VANET: This proposal uses Layer-2 DLT with multi-party (threshold) key management in combination with the leverage of PETs (homomorphic encryption, MPC). The authors focus on the centralized and certificate management deficiencies of current PKI/CA-based methods, suggesting that by redistributing trust, low cost and low latency can be achieved using Layer-2-based distributed identity and key management. Furthermore, concluded with the design provides IPFS/distributed storage at edge; data privacy with PETs and key protection using threshold signatures this paper stressed the importance of 5G/V2X integration and its applications in real world industry like testing.

In the works of Alipanahloo et al. on how to deal with MEV (Maximal Extractable Value)-related unfairness, front-running and network behavior in Ethereum and several L2 solutions by classifying existing mitigation methods in a new taxonomy. The strategies discussed include fair ordering, mempool privacy (threshold/delay encryption, TEE), smart contract-level protection, and Proposer-Builder Separation (PBS), and the effectiveness, latency overhead of censorship resistance and centralization risk for each strategy are analyzed. The rollup/sequencer architecture impact on MEV vs. (assets like TimeBoost, Themis, Helix and MEV-Boost 4). It is pointed out in the paper that delay encryption and PBS are promising, but there still exist some practical issues such as key management, relay centralization and protocol change etc. Finally, the conclusion presents a research road-covering range for future work including shared sequencing and witness encryption.

The study by Chaliasos et al. (2024) offers a theoretical and empirical study of zk-Rollups: Examining implementations (zkleth, zkSync Era) for the ZK-EVM, they consider fixed costs and marginal costs (proof generation, L1 posting, DA bytes etc.) as well as the trade-off between batch size and finality cost with its implications for EIP-4844. The authors note that benchmarking is difficult because of complex prototypes and the absence of common measurements; they present a reproducible and uniform benchmarking process. Ultimately, we determine zk-Rollups provide strong security and high scalability but are not cost-effective in the face of significant economic trade-offs requiring several times longer for proof generation, DA costs and toolchain complexity; instead we suggest improvements to benchmarking infrastructure, formal methods and decentralization around core components (sequencer, prover).

However this point has been particularly emphasized in recent years, with high-profile hacks such as Ronin Network, Poly Network and Mango Markets exposing how DeFi applications need both technical protection and organisational protection. Meanwhile, new design paradigms like Ethereum Layer-2 solutions (Optimism, Arbitrum), Zero-Knowledge rollups (zkSync, StarkNet) and account abstraction (EIP-4337) introduce advances that attempt to increase the level of security. But we should not overlook that they could generate new kinds of vulnerabilities, either.

3. THEORETICAL FRAMEWORK

3.1. The Rise of DeFi and the Security Dilemma

DeFi, in the post-2020 era, Decentralized Finance is one of the most dynamic and innovative of all financial elements after 2020. Such an accelerated growth of the Total Value Locked (TVL) is a strong proof of users' confidence and interest to decentralized applications. The ecosystem is innovative and attractive, and traditional financial transactions (lending, borrowing, providing liquidity on the DEX side or derivative through

smart contracts perform these processes without any central intermediary.

But DeFi has also produced a massive security conundrum. Even though legacy financial institutions transact in a… context with regulatory and oversight frameworks, whereas DeFi operates without such protective architectures— highlighting systemic security issues. This predicament arises from imbalance between rapid innovation and security advancement. It is just in this opening that DeFi allows people to cut out the middleman – in doing so, it exposes the system to attacks by hackers and other bad actors, as well as software bugs.

In theoretical terms, the security/security dilemma distinction can be considered from a transaction cost economics and security dilemma perspective. Centralized structures are more secure but costly; decentralized ones are less expensive. They improve efficiency by cutting out the need for intermediaries. This paradox constitutes a theoretical challenge of critical importance for the long-term sustainability of the DeFi space.

3.2. Sources of Security Vulnerabilities

The security risks relating to DeFi platforms can be attributed to technical, managerial and user-centric aspects. Technically we have reentrancy attacks, oracle manipulations, flash loan attacks and untested smart contracts dominate. These weaknesses are largely due to lack of oversight during fast product development.

Governance issues, despite talking about decentralization, rest in the fact that only few actors are deciding in some projects. The high concentration of token ownership in a handful of whales is against the very philosophy of the democratic governance and poses security threats. This incident demonstrates how the agency cost, a theoretical concept in principal-agent theory where there is conflict of interest and asymmetric information being introduced into DeFi.

User behaviour is also a critical security aspect. Low financial literacy, negligence in private-key safety and wallet management issues make individual investors easy targets. As a result, DeFi security is not just about technical challenges, it's also intimately linked with user behavior.

3.3. Necessity of the Study

The DeFi space is under siege, with billions of dollars in losses. Poly Network, Ronin and Mango Markets are cases that demonstrate a systemic security failure alongside technical ones. This is a situation that poses an existential risk to both investor safety and the longevity of the ecosystem.

The literature review on DeFi security lacks consideration of governance mechanisms, user behaviors and regulatory perspectives: Most studies concentrate on technical aspects. This lack is at odds with the multi-dimensionality of security. Therefore, the significance of this research lies in a holistic security that spans across code, technical, managerial, economic and behavioral.

What's more, DeFi has prompted global concerns among regulators. Money laundering, tax evasion and investor protection constitute the legal and political aspects of DeFi security considerations. Security therefore cannot stop at just technical analysis; there needs to also be practical policy options.

3.4. Contribution of the Study

The study has both academic literature and practical applications. First, case studies are employed in order to concretely locate the causes and effects of security vulnerabilities, which favors theory enlarging with practical incidents.

Secondly, benchmarking the security postures of different DeFi platforms helps in discovering best practices and creates a path for standards to be adopted across the sector. This offers actionable advice to developers and financiers.

Thirdly, a discussion is elaborated on the possible impact of emerging technologies like Ethereum Layer-2 solutions, Zero-Knowledge rollups and account abstraction on DeFi security providing some insights for future work. By this method, not only current but also new emerging hazards will be screened in advance.

Finally, this study presents explicitly the contributions as well as limitations of itself. The study's technical analyses are case studies, not econometric models or economic columns. While providing an opportunity for in-depth concept exploration of the findings, this does restrict generalizability. Nevertheless,

this decision serves the purpose of theoretically locating the topic and constructing a wide-ranging understanding of security.

4. METHODOLOGY

The research is qualitative in nature. Since security vulnerabilities in DeFi ecosystem are multi-factor, quantitative data analysis is not comprehensive. Under these circumstances, the use of a qualitative research design makes room for a broader analysis that comprises technical but also organisational or even behavioural aspects. The research is to complete a full analysis of using literature review, case study and comparison platform review.

The research focuses on four closely-watched hack cases (Ronin Network, Poly Network, Mango Markets and Curve.fi). We chose these cases because they illustrate various forms of attacks in the DeFi landscape, caused financial damage and gained attention in the literature. A few examples include: Ronin and Poly Network (security issues in bridge protocols), Mango Markets (margin and price manipulation) and Curve Finance (compiler related technical mistake). For this reason, we selected the cases to represent a cross-section of DeFi security issues.

The data utilized in the study was acquired from academic papers, industry reports (for example Chainalysis, SlowMist, BlockSec or Sec3) open-source platforms' documentation and independent audit's reports. To verify the reliability of these sources, two datasets were cross-validated using both primary and secondary sources. Additionally, we only utilized public available and verifiable materials. This method is transparent, and reliable results could be obtained.

For both case studies, we employed both content analysis and the comparative case method. We broke down the substance of each attack in (i) the mode of attack, (ii) means by which it was technically carried out, (iii) how our platform responded to it and of course on (iv) the way that it affected its victims. The comparative platform analysis was then conducted, where the security tactics of key DeFi platforms: Aave, Compound, Uniswap, Curve and Synthetix were compared. This analysis was contrasted in relation to the audit policies, insurance mechanisms and governance roles, as well as the technical security measures.

The generalizability of results is, however, restricted due to the qualitative design of the study. In perspective, the cases analyzed only capture a small fraction of the attacks taking place in DeFi. In addition, due to publicly available data this work is based only on data from public sources and not access to closed databases or commercial datasets. This is, however, not an issue that prevents the study from performing a comprehensive conceptual analysis; on the contrary, it is something that aids in grasping the multi-faceted characteristic of DeFi security vulnerabilities.

Table 1. Research Design Overview

Stage of Research Design	Description	Data Output / Purpose
Case selection (Purposeful sampling)	Four large-scale DeFi security incidents were selected based on loss amount, visibility in literature and different vulnerability types (Ronin, Poly, Mango, Curve).	Selection of representative cases covering technical, governance and market manipulation vulnerabilities.
Data collection (Triangulation)	Peer-reviewed papers, independent audit reports, on-chain data, platform documentation (Chainalysis, SlowMist, BlockSec, Sec3).	Cross-validated dataset from academic + industry sources
Data coding (Thematic Analysis)	Open and axial coding performed; codes grouped under three predefined categories: *technical*, *governance*, *user-level vulnerabilities*.	Identification of recurring patterns and vulnerability themes.
Platform comparison (Matrix approach)	DeFi platforms (Aave, Compound, Uniswap, Curve, Synthetix) analyzed based on: audit policy, insurance mechanism, governance model, technical safeguards.	Comparative evaluation revealing differences in platform security posture.

Thematic analysis was employed in the coding process. The authors manually conducted open and axial coding to place them into predefined thematic buckets (technical, governance, and user-level security vulnerabilities). This approach permits pattern identification and comparison across cases and platforms, enabling a systematic treatment of qualitative data.

5. FINDINGS

5.1. Ronin Network Hack (March 2022)

The incident was initiated when the Lazarus Group stole almost all of the validator keys for the Ronin bridge, with 173,600 ETH and 25.5 million USDC then withdrawn before being laundered. As part of this process the stolen funds were tumbled using Tornado Cash, some of the resulting ETH was converted to BTC and then also tumbled once more and eventually cashed out via fiat money services (Chainalysis, 2022).

Decentralization and Centralization within Bridge Protocols The Lazarus Group assault on Ronin bridge shows that centralization in respect to bridge protocols and validator governance is an issue for DeFi when addressing security. As discussed in the Chainalysis (2022) report, the washing of stolen funds via Tornado Cash and other mixing services demonstrates that the current anti-money laundering (AML) tools can be ineffective in DeFi. Academically, this case once again suggests the necessity of provable audits, multi-signature checks and open monitoring systems in cross-chain transaction and bridge architecture; it also highlights the importance of making DeFi protocols more immune to financial crimes.

5.2. Poly Network Hack (August 2021)

Cross-chain interoperability protocol Poly Network was hacked on August 10, 2021 via a critical vulnerability. As per SlowMist's research, the exploit exploited the verifyHeaderAndExecuteTx method of the EthCrossChainManager contract. The fact that this function could call putCurEpochConPubKeyBytes of the EthCrossChainData contract enabled the attacker to point the guardian role of said contract's instance to his own address. This allowed the attacker to drain funds from the contract via illicit transaction validation. This serves as exemplification to highlight the importance of governance and validation mechanisms in security for cross-chain protocols (SlowMist, 2021).

The Poly Network hack, on August 10th, 2021 is a lesson that design errors in interchain protocol governance and verification processes can have disastrous financial consequences. The changing of guardian role via EthCrossChainManager contract allowed the attacker to take over the whole system, and it is a clear demonstration that just one security issue in smart contracts can result in loss of billions of dollars. From an intellectual standpoint, this episode shows that bridge protocols in the DeFi system must be required to include formal proving methods, multi-signature solutions, independent security audits etc. In addition, revealing and auditing the cross-chain interaction mechanism to prevent such attack provides an increasingly mandatory requirement in the literature.

5.3. Mango Markets Exploit (October 2022)

The attacker put 10m USDC into two accounts through FTX to create two Mango accounts as collateral during the 2022 assault on Mango Markets. Using these accounts, the hacker used a large long and short on MNGO-PERP futures to manipulate the spot prices on the Serum DEX; this had developed over time into a chain driving up the price of an MNGO token from 0.382 USDC to 0.5 USDC (a 13x increase). The attacker took advantage of PnL (Profit and Loss) calculation between accounts to create over 200M unrealized profits on MangoAccount1 and leverage this account to borrow and withdraw BTC, USDT, SOL mSOL, USDC (worth about 120M USD in total) within a few minutes. The event demonstrates the possibility of abusing margin/leverage on Mango's futures trading platform and also how volatile tokens can be (Sec3, 2022).

The recent Mango Markets exploit highlights that margin and leverage mechanisms in decentralized finance (DeFi) have potential systemic risks. The fact that an attacker can quickly take such significant profits for themselves by manipulating prices in unregulated liquidity pools and protocols based on token volatility demonstrates how serious are the risks which these systems can pose. From an intellectual point of view, this incident demonstrates the need to enhance automated risk-management systems and margin/leverage cap limitations as well as oracle-relying price verification machineries work on DeFis. Moreover, strengthening the robustness of protocols against flash-bots is key for investor protection as well as ecosystem stability.

5.4. Curve Finance Exploit (July 2023)

A vulnerability analysis from BlockSec dated 2024, revealed the origin of growth finance attack is bug in vyper compiler. The vulnerability made reentrancy protection of smart contracts not work, and these

included contracts compiled using Vyper versions 0.2.15, 0.2.16 and one beta version 0.3.0. The reason is that locks reentrant in different functions are written to different positions. This scenario illustrates how issues in a compiler can lead to severe and subtle attacks on the security and robustness of blockchain systems. From a research perspective, this incident emphasizes the absolute necessity of secure compilers for DeFi protocol safety and stresses the importance of thorough audits, bug bounty programs, and the construction of automated attack detection/prevention mechanisms (BlockSec, 2023).

The attack on Curve Finance is a stark example that technical underpinning weaknesses in the DeFi sector pose systemic risks. Compiler-related security issues can result in incorrect operation of smart contacts, potentially causing huge monetary losses for protocols. From a research standpoint, this is yet another indicator that these DeFi protocols need to be carefully examined not just for contract code but also the security of the compilers with which they are created. There are also measures such as automatic security scans, deep review processes and the extensive use of bug bounty programs that play an important role in protecting protocols from technical errors.

5.5. Comparative Analysis of the Cases

These four examples – Ronin Network, Poly Network, Mango Markets and Curve Finance – all showcase distinct issues that permeate the DeFi space. While there are unique vulnerabilities in each case, patterns of weak governance, inadequate oversight and a lack of technological preparedness also emerged. For enhanced comparison of these similarities and differences, a table of comparative summary of the reported cases has been added.

Table 2. Selected DeFi Attack Cases: Vulnerability Types, Financial Losses and Key Lessons

Case	Type of Vulnerability	Amount of Loss (USD)	Primary Cause	Key Lesson
Ronin	Validator management	~$625 M	Centralized architecture	Multi-signature controls; transparent governance
Poly Network	Governance flaw	~$600 M	Smart-contract manipulation	Formal verification; independent audits
Mango Markets	Oracle/manipulation	~$120 M	Margin & leverage abuse	Automated risk management; oracle-diversity
Curve Finance	Compiler bug	~$70 M+	Vyper-origin technical error	Compiler security; bug bounty programs

As these four cases illustrate, the risks are serious at every layer of DeFi protocols, from validator management, to market structure design, slippage attacks and compiler level bugs. Thus, to be secure it is not sufficient (but merely necessary) to perform an audit of smart contracts; the compilers, oracles and governance models must also undergo inspection. Automated risk management systems, multi-signature verification implementations allowing signers to verify transactions before signing for them, robust audits and generous bug bounties are not only key to creating resilience against technical failures but also provide a good line of defence against financial threats.

6. DISCUSSION AND PROPOSED SOLUTIONS

Through the examination of these cases, we demonstrate that DeFi security issues are not limited to technical vulnerabilities, but are also determined by governance mechanisms, user activities and gaps in regulation. Every incident demonstrated that low points in these dimensions can lead to massive losses, reduce investor confidence and increase systemic risk to any cryptocurrency ecosystem at large.

To cope with these challenges, this section presents solution directions in four dimensions: audit policies, insurance solutions, governance and open management solutions, technical defense solutions. A comparative view on top DeFi platforms— Aave, Compound, Uniswap, Curve and Synthetix is presented in the table below, followed by more detailed investigation on each dimension.

Table 3. Comparative Overview of Audit, Insurance, Governance, and Technical Safeguards in Leading DeFi Platforms

Platform	Audit Policy	Insurance Mechanism	Governance & Open Management	Technical Safeguards
Aave	Independent audits + bug bounty	Integrated with Nexus Mutual	DAO-based governance	Oracles, reentrancy guard
Compound	OpenZeppelin audit	None	Token-based governance	Governor timelock, upgrade protections
Uniswap	Open-source, audits	None	GitHub + token-based voting	Minimal code, immutable contracts
Curve	Audited, but low frequency	Partial protection	Community + GitHub contributions	Stablecoin pool optimizations
Synthetix	Continuous audits + insurance fund	Internal pool	Decentralized voting	Oracle security, collateral requirements

6.1. Audit Policies

Audit procedures are one of the basic aspects to increase the trustworthiness on DeFi. For instance, Aave and Synthetix both perform regular independent audits and have bug bounty programs that lead to the proactive detection of security holes. By comparison, audits for Curve have been few and far between and that's come with some major risks, illustrated by the reentrancy attack.

The need for continuous and layered auditing is apparent. Rather than single-point security, repeated cross-audits are more secure overall. Another factor is systems where the community is motivated to participate, such as programs that offer bounties for vulnerabilities before they are discovered by the bad guys. This means that outside experts, as well as us users, have a say in creating network security that should function like an onion.

6.2. Insurance Mechanisms

There are insurance schemes that is protecting users' funds. Examples of such integrations would be Aave's integration with Nexus Mutual, or Synthetix's in-house insurance pool. Meanwhile, the failure to offer insurance products on platforms like Compound and Uniswap kills user trust.

Transparency in reserves level, independent audits and automated compensation protocols are important for the sustainability of insurance mechanisms in DeFi. DeFi insurance is community driven as opposed to the standard model of insurance and generally have a voting element. This does increase transparency, but also opens bottlenecks for potential manipulation and low participation. So trust over the long term is a function not only of the size of the pools but also of having risk assessments based on objective measures.

6.3. Governance and Open Management

DAO-based governance frameworks (such as Aave, Synthetix) increase transparency, but a few shareholders can control decision-making. In Compound and Uniswap, even token-based governance can be weaponized. Curve, for its part, is very community oriented but the decision-making process can be slow and inefficient.

Good governance necessitates multiple layers and levels of voting, quotas for small investors, and long-term lockups (staking) in governance tokens. In addition, an open policy of managing things in which platforms regularly report on their decisions can nurture trust with users. Enacting such measures, DeFi platforms can reinforce not only their technical security, but democratic inclusivity as well.

6.4. Technical Security Measures

Some of the popular types of DeFi attacks are Oracle attack, flash loan hack and compiler vulnerability. As we observed in the case of Mango Markets, price manipulations could result not only from glitches in code but also because of defect designs of markets. The compiler security became even more obvious with the Curve Finance exploit.

Hence, developing multi-source oracle systems, anomaly detection agents and formal verification of compilers is essential. A multi-signature environment, cross-chain bridge decentralization, hardware-based security, and bug bounty programs are some of the keystone technical security aspects in DeFi.

The comparative analysis reveals that large variations exist in security of adopted strategies among the assessed DeFi platforms. Differences in audit frequency, integration with insurance, and governance directly impact security against attacks. Aave and Synthetix reveal more holistic security models, but for Compound and Uniswap, being not insured or broadly audited shows are still exposed.

6.5. Ethereum Layer-2 Technologies (Optimism, Arbitrum)

Layer 2 is one of the most adopted approaches to tackle blockchains scalability issues. They solve this problem by allowing transactions to be carried out off-chain and offering just the summarized outcome to the main chain, thus diminishing network load and transaction time (Sguanci, et al., 2021). These Layer-2 solutions are developed to address Ethereum's high gas fees and constrained ability to accommodate transactions. Rollup-based solutions like Optimism and Arbitrum scale by performing transactions off-chain, but settle everything back to the mainnet. This enables faster, more cost-effective, and therefore more widespread use of DeFi dApps.

Layer-2 solutions, however, open up new security debates as well. Especially, centralized bridge nodes are the hot targets for attackers. The Ronin and Poly Network hacks showed that bugs in bridges can result in losses of billions of dollars. Furthermore, as some operations are executed off-chain, validation could be plagued by lack of transparency. So long-term success of Layer-2 solutions is a question not only of technical performance, but also the extent that solid security and clear governance can be incorporated.

6.6. Zero-Knowledge Rollups (zk-Rollups)

Zk-Rollups has become one of the more promising approaches for achieving scalability and privacy simultaneously on blockchain. By applying zk-Rollups for the aggregation of several transactions, a significantly higher throughput and lower costs can be achieved on the main chain (Torralba-Agell et al., 2024). Because they process transactions off-chain, execution speeds increase and systems like zkSync and StarkNet mathematically verify transaction validity and store only necessary data on-chain. This is advantageous in that it allows high capacity to be achieved, with security of data.

However, the high technical complexity of zk-Rollups brings two risks along for the ride. On the one hand, zero-knowledge proofs are inherently strong; on the other, if there is a coding error or nano-audit and testing of code may leave these systems with holes. As zk-Rollups are one of the newer technologies, their security guarantees continue to mature. For this to be the case, formal verification with extensive testnet testing and audits, including independent ones are must-haves.

6.7. Smart Wallets and Account Abstraction (EIP-4337)

The integration of EIP-4337 by the Ethereum community is a significant advance both in terms of user experience and security. EIP-4337 account abstraction allows features such as gas sponsorship by smart contracts and ERC-20 payments of transaction fees (Sahu, et al., 2023). Users can also delegate gas costs, specify recovery plans, and use multi-factor authentication using this model. Hence, some problems like losing the private key, the transaction is not arrived at destination and high gas fee will be alleviated to a great extent.

Account abstraction can even drive institutional traction for DeFi. It lowers the technical barrier for users to participate through better user protection and allows users to interact easily with smart contracts. Furthermore, the compatibility of different blockchain systems can contribute to ecosystem creation (Wang and Chen, 2023). For businesses and big investors, multi-sig security measures, hardware strategies and transaction flexibility ensure you're not taking unnecessary risks, giving you more peace of mind when investing. However, since the model is currently adopted, it suffers from the normative barrier. Therefore, the smooth roll-out of EIP-4337 depends on cooperation between wallet developers, audit companies, and user groups.

6.8. Integrated DeFi Security Framework (IDSF)

Based on findings of case analyses and emergent codes from the thematic coding, we propose in this study the Integrated DeFi Security Framework (IDSF). In contrast to earlier work that only concerned with technical security vulnerabilities, the IDSF encompasses DeFi security as a more complex system that is influenced by interactions across technical, governance and user aspects. The three distinct levels at which vulnerabilities are introduced do not result in independent security breaches; rather they influence the aggregated behaviour among the three power levels.

Table 4. Integrated DeFi Security Framework (IDSF)

Security Layer	Type of Vulnerability	Mechanism / Root Cause	Recommended Solution Strategy
Technical Layer	Smart contract bugs, compiler errors, oracle manipulation, flash-loan attacks	Code complexity, low audit frequency, insufficient testing	Formal verification, multi-source oracle design, continuous audits, bug bounty programs
Governance Layer	Token ownership concentration, centralized validators/bridges, weak voting accountability	Governance capture by whales, single point of failure	DAO transparency, multi-sig validators, voting safeguards, bridge decentralization
User Layer	Private key loss, phishing, wallet misuse, lack of financial literacy	Insufficient user security design, complex irreversible errors	Account abstraction (EIP-4337), wallet recovery models, UX-focused security prompts, user education

The IDSF model shows that a technical audit isn't enough to secure DeFi systems. Three concurrent interventions must be leveraged for a sustainable security:

(1) improve the protocol infrastructure with formal verification and multi-source oracles,

(2) decentralized governance with elucidated decision-making power and multi-signature validator mechanisms,

(3) user protection through smart wallet recovery processes (EIP-4337) — this one is to prevent users from the illusion that a system they count on will always be secure; it's only possible with UX-based security measures, not by "patching" existing security.

As such, security in DeFi can't simply be solved with technical measures and coding fixes, but requires an integrated approach between technology, governance and how users behave in the system.

In contrast to prior works, IDSF yields a holistic and generic DeFi security model that can be used for both current and upcoming DeFi systems. This, alongside its focus on Layer-2 rollups, Zero-Knowledge and account abstraction levels, helps to provide a more structured scaffolding for developers and regulators that will inevitably need to be contended with as they work to resolve tomorrow's DeFi security issues.

In doing so, IDSF eliminates siloed DeFi security efforts and replaces them with an integrated, multi-layer security model that can serve as the foundation for building a better and more sustainable DeFi.

7. CONCLUSION

This work presented a comprehensive analysis of the different weaknesses in the security of DeFi and offered recommendations on technical, governance and user fronts. The results indicated that the risks include not only coding bugs in smart contracts, but also reliance on oracles, flash loan attacks, centralized bridges and inadequate governance structures. And the high-profile cases have shown that these weaknesses easily lead to losses in the tens of billions and, therefore, put investor protection and systemic stability at risk.

The findings suggest three priority areas:

1. Technical defenses well-audited defenses and formally verifiable safeguards through formal verification, automated testing, bug bounties.
2. Broader provision of insurance and risk-transfer instruments to offset user loss and improve resilience.
3. Exposing greater transparency and inclusiveness in centralized parts such as bridges or token-based governance models.

Lack of Regulation Meanwhile, the absence of regulation has been cited as a seriously compromising factor in DeFi security. Internationally harmonised frameworks at the very least, much like those already established in regulatory systems like AML and KYC, could give the system with legal legitimacy that would in turn may increase investor confidence.

New technologies appear to promise possibilities in this respect. Layer-2 lowers transaction costs; zk-Rollups give you scaling and privacy at the same time; EIP-4337 takes security and UX to a new level. But these technologies have risks, which should be reduced via independent audits, long-running testnet trials and clear governance mechanisms before they are deployed.

The major contribution of this research is the construction of IDSF (Integrated DeFi Security Framework), that regards DeFi security as not a simple technical coding problem, but as a multidimensional framework involving technical issue, governance and user. Compared to previous works providing isolated points of view, IDSF provides a complete perspective that shows which security mechanisms have to be adopted in every level.

The model provides developers, investors and policy-makers with an implementation route by mapping sources to take action upon against potential means to reduce their vulnerability. So, this paper adds to the literature by providing a conceptual security model to guide future research and reinforce the sustainability of decentralized finance ecosystems.

In conclusion, the future of DeFi relies on its technology as well as an integrated approach to security, proactive regulation and a higher degree of user education. This research adds to the knowledge base by offering policy and industry implications. Further study could pay attention to the formal verification method development, MEV attacks resistance mechanisms construction, user-oriented interface design optimization and insurance mechanism designing in low-fee blockchain networks.

Ethics Committee Declaration

Ethics committee declaration is not required for the study.

Author Contribution Rate Declaration

This study was entirely conducted and written by Batuhan Karabay.

Conflict Statement

There is no conflict of interest between the authors.

Declaration of Support

No support was received from any organization for this study.

REFERENCES

Adarbah, A., Tolba, A., Belattar, B., and Moulad, M. (2024). Blockchain-Assisted Security and Privacy Preservation Scheme for Vehicular Ad Hoc Networks. *Security and Privacy, 7*(4), e307. https://doi.org/10.1002/spy2.307

Alipanahloo, Z., Hafid, A. S., and Zhang, K. (2024). Maximal Extractable Value Mitigation Approaches in Ethereum and Layer-2 Chains: A Comprehensive Survey. *ArXiv Preprint, arXiv:2407.19572*. Retrieved May 03, 2025, from https://arxiv.org/abs/2407.19572

BlockSec. (2024, February 14). *Curve incident: Compiler Error Produces Faulty Bytecode from Innocent Source Code.* BlockSec Blog. Retrieved April 16, 2025, from https://blocksec.com/blog/curve-incident-compiler-error-produces-faulty-bytecode-from-innocent-source-code

Chainalysis. (2022, September 8). *$30 million seized: How the cryptocurrency community is making it difficult for North Korean hackers to profit.* Chainalysis Blog. Retrieved May 08, 2025, from https://blog.chainalysis.com

Chaliasos, S., Reif, I., Torralba-Agell, A., Ernstberger, J., Kattis, A., and Livshits, B. (2024). Analyzing and Benchmarking zk-Rollups. In *6th Conference on Advances in Financial Technologies (AFT 2024)* (pp. 6–1). Schloss Dagstuhl—Leibniz-Zentrum für Informatik.

Li, W., Bu, J., Li, X., Peng, H., Niu, Y., and Zhang, Y. (2022). A survey of DeFi security: Challenges and Opportunities. *Journal of King Saud University—Computer and Information Sciences,* 34(10), 10378–10404. https://doi.org/10.1016/j.jksuci.2021.10.020

Qin, K., Zhou, L., Livshits, B., and Gervais, A. (2021). Attacking the DeFi ecosystem with flash loans for fun and profit. In *International Conference on Financial Cryptography and Data Security* (pp. 3–32). Springer.

Roșca, I., Butnaru, A.-I., and Simion, E. (2023). Security of Ethereum Layer 2s. *IACR Cryptology ePrint Archive,* 2023(124). Retrieved April 26, 2025, from https://eprint.iacr.org/2023/124

Sahu, N., Gajera, M., and Chaudhary, A. (2023). ZkFi: Privacy-Preserving and Regulation Compliant Transactions Using Zero Knowledge Proofs. *ArXiv Preprint, arXiv:2307.00521*. Retrieved April 28, 2025, from https://arxiv.org/abs/2307.00521

Sec3. (2022, October 13). *How to analyze an attack? A Case Study on The Mango Markets exploit.* Sec3 Blog. Retrieved April 13, 2025,

from https://www.sec3.dev/blog/mangoexploit

Sguanci, C., Spatafora, R., and Vergani, A. M. (2021). Layer 2 Blockchain Scaling: A Survey. *ArXiv Preprint, arXiv:2107.10881*. Retrieved July 28, 2025, from https://arxiv.org/abs/2107.10881

SlowMist. (2021, August 10). *The root cause of Poly Network being hacked.* Medium. Retrieved May 03, 2025, from https://slowmist.medium.com/the-root-cause-of-poly-network-being-hacked-ec2ee1b0c68f

Torralba-Agell, A., Keshavarzkalhori, G., Pérez Solà, C., Megías, D., and Herrera Joancomartí, J. (2024). Unmasking the illusion: The shortcomings of "zero-knowledge" rollups in achieving privacy. In *XVIII Reunión Española sobre Criptología y Seguridad de la Información: XVIII RECSI* (pp. 361–366).

Wang, B., Liu, H., Liu, C., Chen, X., Liu, Z., Sun, L., and Zhang, T. (2021). BLOCKEYE: Hunting for DeFi attacks on blockchain. *ArXiv Preprint, arXiv:2103.02873*. Retrieved May 11, 2025, from https://arxiv.org/abs/2103.02873

Wang, Q., and Chen, S. (2023, December). Account abstraction, analysed. In *2023 IEEE International Conference on Blockchain (Blockchain)* (pp. 323–331). IEEE. https://doi.org/10.1109/Blockchain57800.2023.00054