Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Next-Generation Security Architecture for DeFi Platforms: A Framework for Global Financial Resilience

Gresshma Atluri
Cybersecurity & Risk Consultant at The World's 3rd Largest Oil & Gas Giant

ARTICLE INFO

Received: 12 July 2025

Revised: 11 Aug 2025

Accepted: 20 Aug 2025

ABSTRACT

This paper introduces a pioneering multi-layered cybersecurity framework for Decentralized Finance (DeFi) platforms, fundamentally transforming traditional financial infrastructure by operating without centralized intermediaries through blockchain-based smart contracts, creating unprecedented accessibility while simultaneously introducing complex security challenges requiring specialized defense mechanisms. The immutable nature of blockchain technology necessitates comprehensive proactive security measures, as deployed smart contracts cannot be easily modified to address discovered vulnerabilities. Multi-layered security frameworks encompass pre-deployment foundations, including rigorous smart contract auditing by multiple independent firms, formal verification processes that mathematically prove contract behavior alignment with intended specifications, and transparent code documentation enabling thorough community security reviews. Runtime protection mechanisms incorporate time-locks enforcing mandatory delays before implementing critical protocol changes, circuit breakers serving as emergency stops when suspicious activity is detected, and rate limiting controls preventing flash loan attacks through transaction volume restrictions. Access control systems utilize multi-signature wallets requiring multiple authorized parties for transaction approval, while progressive decentralization strategies enable structured transitions from centralized development teams to distributed community governance. Financial protection frameworks integrate insurance protocols providing coverage against successful exploits, treasury management systems maintaining reserve funds through secure multi-signature mechanisms, and comprehensive risk management frameworks enabling continuous monitoring and threat identification. Community-driven security initiatives leverage distributed expertise through bug bounty programs offering competitive rewards for responsible vulnerability disclosure, collaborative security reviews identifying issues missed by formal auditing, and educational programs enhancing user awareness of security best practices and threat recognition capabilities.

Keywords: decentralized finance security, smart contract auditing, multi-signature wallets, bug bounty programs, formal verification, runtime protection mechanisms

Introduction

Decentralized Finance platforms represent a fundamental transformation in financial infrastructure, operating without traditional intermediaries through blockchain-based smart contracts. Such innovation delivers unprecedented accessibility and programmability to financial services, while simultaneously introducing distinct security challenges requiring specialized defense mechanisms. The immutable nature of blockchain technology means that once deployed, smart contracts cannot be easily modified to fix vulnerabilities, making proactive security measures absolutely critical. The high-stakes environment of DeFi, where billions of dollars in value are managed by autonomous code, has made these platforms attractive targets for malicious actors seeking to exploit weaknesses in protocol design or implementation.

The emergence of DeFi has fundamentally altered the landscape of financial services by eliminating the need for traditional financial intermediaries such as banks, brokers, and exchanges. DeFi protocols operate through smart contracts that automatically execute financial transactions when predetermined conditions are met, creating a trustless environment where participants can engage in lending,

Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

borrowing, trading, and yield farming without relying on centralized authorities [1]. The programmable nature of smart contracts enables the creation of complex financial instruments and strategies that would be impossible or prohibitively expensive to implement in traditional finance systems.

The rapid expansion of the DeFi ecosystem has created an environment where security vulnerabilities can result in catastrophic financial losses affecting millions of users worldwide. The decentralized architecture of these platforms introduces unique attack vectors that differ fundamentally from traditional financial systems, where security breaches can be contained through administrative controls and regulatory oversight. DeFi protocols operate autonomously once deployed, making post-deployment security modifications extremely challenging or impossible without complete protocol redeployment [1].

Smart contract vulnerabilities have been systematically categorized into several distinct types, each requiring specific defensive strategies to mitigate potential exploitation. Deep learning-based vulnerability detection tools have emerged as sophisticated solutions for identifying security weaknesses in Ethereum smart contracts, utilizing advanced machine learning algorithms to analyze code patterns and detect potential vulnerabilities before deployment. These automated detection systems can identify common vulnerability patterns, including reentrancy attacks, integer overflow conditions, access control failures, and oracle manipulation scenarios [2].

The complexity of attack vectors is compounded by the composability of DeFi protocols, where interactions between multiple smart contracts can create unexpected vulnerabilities that emerge only through complex transaction sequences. The transparent nature of blockchain technology means that successful attacks are immediately visible to the entire network, often triggering cascading effects across interconnected protocols. Such transparency, while beneficial for accountability purposes, also provides malicious actors with complete visibility into protocol mechanics and potential attack vectors, necessitating defense mechanisms that assume complete information disclosure to adversaries.

Pre-Deployment Security Foundations

The foundation of DeFi security begins long before a protocol goes live, with comprehensive smart contract auditing serving as the primary defense mechanism. Multiple independent security firms should examine the codebase to identify potential vulnerabilities, as different auditing teams often discover distinct issues due to varied methodologies and expertise. The multi-layered approach significantly reduces the likelihood of critical vulnerabilities reaching production environments.

Smart contract auditing has evolved into a sophisticated discipline requiring specialized expertise in blockchain technology, cryptography, and financial protocol design. Professional auditing firms employ systematic methodologies that combine automated analysis tools with manual code review processes to identify potential security vulnerabilities. Static analysis techniques have emerged as fundamental components of smart contract security assessment, particularly for detecting transaction conflicts and race conditions that can lead to exploitable vulnerabilities. Advanced static analysis frameworks can systematically examine smart contract bytecode and source code to identify potential security issues without requiring contract execution, making such tools invaluable for pre-deployment security verification [3].

The implementation of static analysis for smart contract security has become increasingly sophisticated, with specialized tools designed to detect specific categories of vulnerabilities, including transaction conflicts, reentrancy attacks, and state inconsistencies. Static analysis methods can examine smart contract implementations to identify potential race conditions where multiple transactions might interfere with each other, potentially leading to unexpected behavior or security vulnerabilities. The analysis process involves constructing control flow graphs and data dependency models that represent all possible execution paths within smart contracts, enabling comprehensive vulnerability detection across complex protocol implementations [3].

Formal verification represents the mathematical pinnacle of smart contract security, providing mathematical proof that contract behavior aligns with intended specifications. The process involves

Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

creating mathematical models of contract logic and using automated theorem provers to verify that all possible execution paths behave as expected. While resource-intensive, formal verification can catch subtle logical errors that traditional auditing might overlook, particularly in complex protocols involving intricate mathematical operations or state transitions. The formal verification ecosystem for smart contracts has expanded significantly, with multiple frameworks and methodologies available for different verification requirements and complexity levels [3].

Code documentation and transparency play crucial roles in the security ecosystem, enabling more thorough security reviews and helping identify potential attack vectors that might not be immediately apparent. Open-source development allows the broader security community to contribute to identifying vulnerabilities, creating a collaborative defense mechanism that extends beyond paid auditing services. The evolution of smart contract frameworks has demonstrated the importance of comprehensive documentation and standardized development practices for maintaining security across diverse applications. Survey research indicates that smart contract frameworks encompass various architectural approaches, from simple transaction processing systems to complex decentralized applications supporting multiple programming languages and deployment environments [4].

The collaborative nature of open-source security research has led to the development of specialized tools and frameworks designed to facilitate community-driven vulnerability discovery. Smart contract frameworks have diversified to support different blockchain platforms, programming languages, and application requirements, with each framework offering distinct security features and development methodologies. The proliferation of smart contract frameworks has created a rich ecosystem where developers can choose appropriate tools based on specific security requirements, performance constraints, and functional specifications [4].

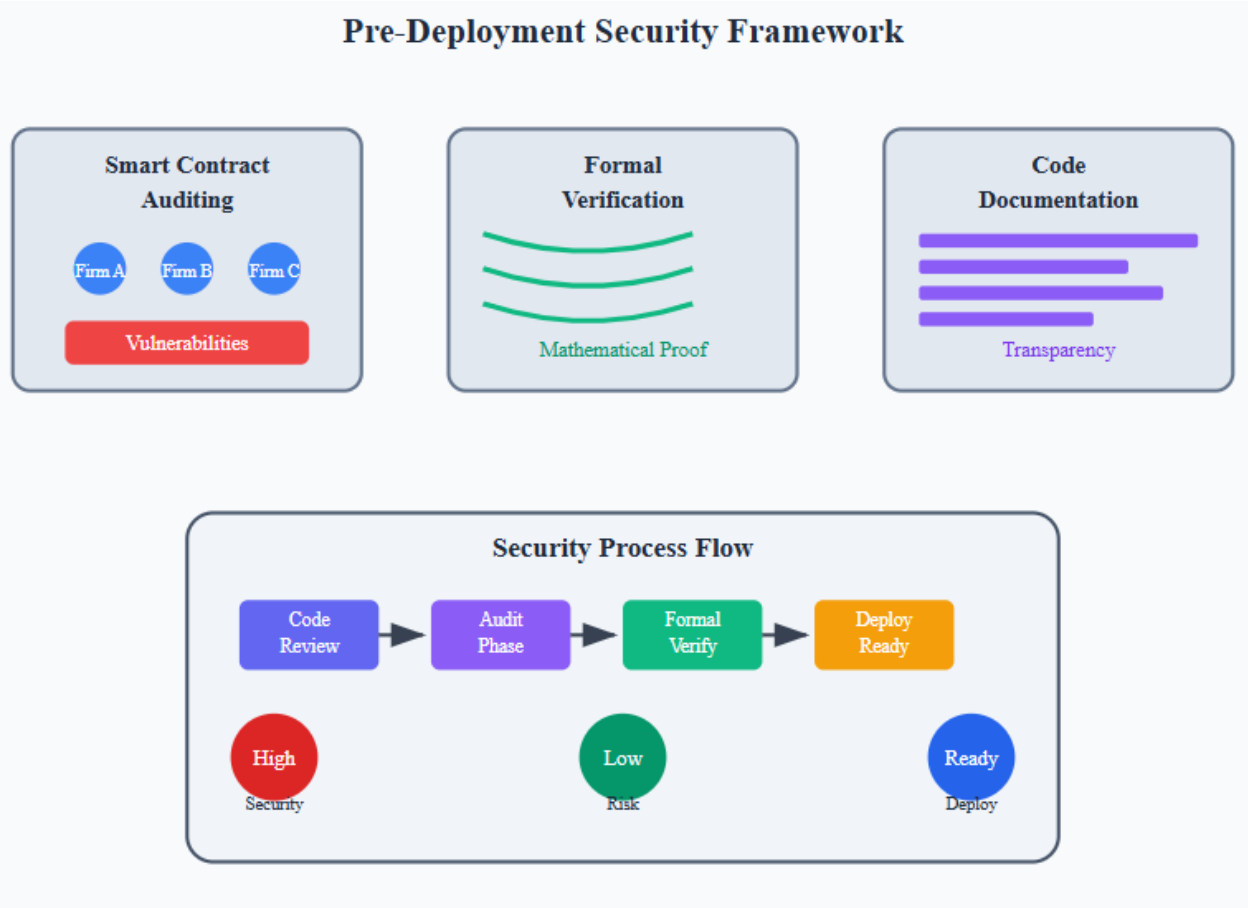

Fig 1. Pre-Deployment Security Framework [3, 4].

Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Runtime Protection Mechanisms

Once deployed, DeFi protocols require active defense mechanisms to protect against real-time threats. Time locks serve as critical safety mechanisms by enforcing mandatory delays before implementing significant protocol changes. These delays provide community members and security researchers sufficient time to analyze proposed modifications and identify potential security implications before becoming active.

Time-lock mechanisms have emerged as fundamental security components in DeFi protocol governance, establishing mandatory waiting periods that range from several hours to multiple days, depending on the significance of proposed changes. The implementation of time locks creates a temporal buffer zone where protocol modifications undergo community scrutiny before execution, enabling stakeholders to identify potential security vulnerabilities or malicious proposals. Advanced time-lock systems incorporate multi-signature requirements and hierarchical approval processes that ensure critical protocol changes receive adequate review from multiple independent parties. Flash loan attacks have demonstrated the critical importance of temporal safeguards, with research showing that attackers can exploit protocol vulnerabilities within single blockchain transactions, making time locks essential for preventing instantaneous exploitation of newly discovered vulnerabilities [5].

Circuit breakers act as emergency stops that can halt protocol operations when suspicious activity is detected. These mechanisms monitor key metrics such as unusual transaction volumes, rapid price movements, or unexpected contract interactions. When predetermined thresholds are exceeded, circuit breakers can temporarily pause operations, preventing further damage while allowing time for investigation and response. The sophistication of circuit breaker systems has evolved to incorporate real-time monitoring capabilities that can detect anomalous patterns in transaction behavior, enabling proactive threat detection before significant damage occurs. Flash loan exploitation patterns have revealed that attackers often execute complex multi-step transactions involving price manipulation and arbitrage opportunities, with some attacks generating profits exceeding $1 million within single transactions [5].

Rate-limiting mechanisms protect against flash loan attacks and other high-frequency exploits by restricting transaction volumes within specific time windows. These controls prevent attackers from manipulating protocol state through rapid, large-volume transactions that exploit temporary price discrepancies or liquidity imbalances. The design of effective rate-limiting systems requires careful consideration of legitimate user behavior patterns to avoid restricting normal protocol operations while maintaining protection against malicious activities. Analysis of flash loan attack vectors demonstrates that successful exploits often involve borrowing substantial amounts of cryptocurrency without collateral, with attack volumes sometimes exceeding hundreds of millions of dollars in borrowed funds within single transactions [5].

The implementation of runtime protection mechanisms has become increasingly sophisticated, incorporating real-time monitoring systems that analyze transaction patterns, liquidity flows, and market conditions to detect potential threats. DeFi protocols operate as interconnected ecosystems where smart contracts automatically execute financial transactions without traditional intermediaries, creating environments where automated lending, borrowing, and trading occur continuously across multiple platforms. The decentralized nature of these systems enables users to participate in complex financial activities, including yield farming, liquidity provision, and automated market making, with total value locked in DeFi protocols reaching substantial amounts across numerous blockchain networks [6].

The effectiveness of runtime protection mechanisms depends heavily on proper calibration and continuous monitoring to ensure optimal performance across diverse market conditions. Modern DeFi protocols implement adaptive protection systems that can modify response thresholds based on real-time risk assessments and market volatility indicators. The continuous evolution of attack vectors necessitates regular updates to protection mechanisms, with successful protocols implementing

Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

automated monitoring systems that can detect and respond to new threat patterns without manual intervention [6].

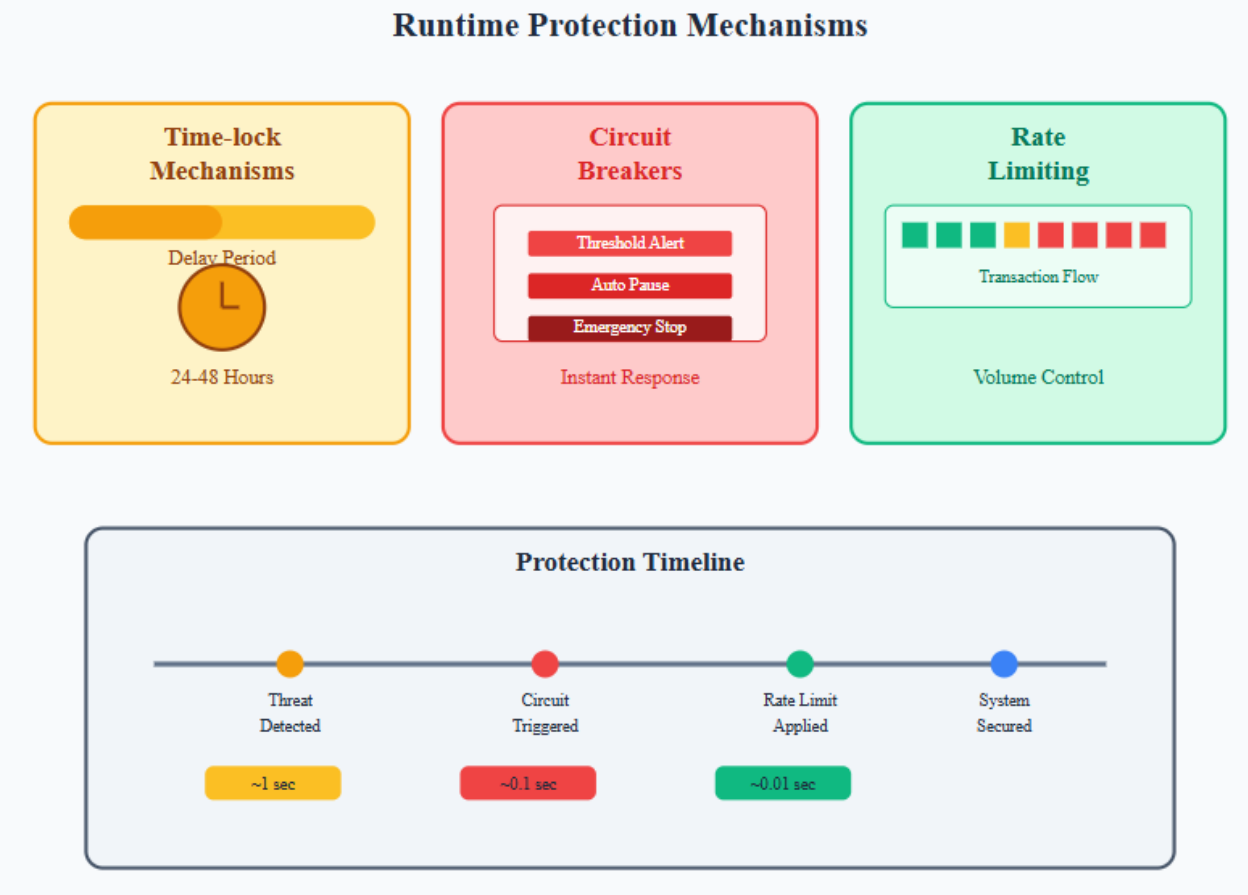

Fig 2. Runtime Protection Mechanisms [5, 6].

Access Control and Governance Security

Multi-signature wallets represent a fundamental security improvement over single-key control systems by requiring multiple authorized parties to approve critical transactions. The distributed control mechanism eliminates single points of failure and makes it significantly more difficult for malicious actors to compromise protocol operations. The threshold requirements for multi-signature approvals should be carefully calibrated to balance security with operational efficiency.

Multi-signature wallet implementations have evolved into sophisticated security frameworks that distribute control across multiple stakeholders, creating robust defense mechanisms against unauthorized access and malicious activities. The mathematical foundation of multi-signature systems relies on threshold cryptography, where a minimum number of signatures from a predefined set of authorized parties must be collected before transaction execution can proceed. Advanced multi-signature schemes incorporate hierarchical access controls that assign different permission levels to various participants, enabling fine-grained control over protocol operations while maintaining security through distributed authority. Comprehensive analysis of Ethereum smart contract security reveals that access control vulnerabilities represent one of the most critical categories of security issues, with improper access control implementations accounting for a significant percentage of successful attacks on DeFi protocols [7].

Progressive decentralization offers a structured approach to transitioning control from centralized development teams to distributed community governance. The gradual process allows protocols to maintain necessary security controls during the early stages while eventually achieving true decentralization. The transition must be carefully managed to ensure that decentralization does not

Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

compromise security or introduce new attack vectors through governance token manipulation. The implementation of progressive decentralization typically involves multiple phases, beginning with core development team control and gradually transferring authority to community-controlled governance mechanisms. Smart contract security research indicates that governance-related vulnerabilities have become increasingly prominent as DeFi protocols implement more complex governance mechanisms, with security tools now specifically designed to detect governance manipulation attacks and access control bypasses [7].

Governance token security involves protecting the voting mechanisms that control protocol evolution. Time-locked voting periods prevent sudden governance attacks, while delegation mechanisms allow token holders to participate in governance without exposing holdings to unnecessary risk. The design of secure governance systems requires careful consideration of token distribution patterns, voting power concentration, and potential attack vectors that could enable malicious actors to manipulate protocol decisions. Advanced governance frameworks incorporate quadratic voting mechanisms and reputation-based systems that prevent concentrated token holdings from dominating decision-making processes. The current state of smart contract security tools includes specialized frameworks designed to analyze governance token implementations and detect potential vulnerabilities in voting mechanisms and delegation systems [7].

The evolution of decentralized governance has created complex ecosystems where token holders participate in protocol decision-making through various mechanisms, including proposal submission, voting, and delegation. Governance tokens serve multiple functions within DeFi protocols, acting as both voting instruments and economic incentives that align participant interests with protocol success. The distribution and concentration of governance tokens significantly impact protocol security, with highly concentrated token holdings potentially enabling governance attacks where malicious actors acquire sufficient voting power to manipulate protocol parameters. Research indicates that DeFi protocols have fundamentally transformed traditional financial intermediation by enabling direct peer-to-peer transactions without requiring trusted third parties, creating new governance challenges that require innovative security solutions [8].

The security of governance mechanisms depends heavily on the proper implementation of voting procedures, delegation frameworks, and proposal evaluation processes. Modern governance systems incorporate sophisticated mechanisms for proposal evaluation, including technical review processes, community discussion periods, and multi-stage voting procedures that ensure thorough consideration of proposed changes. The integration of governance tokens with DeFi protocols creates complex interdependencies where token price movements can influence governance participation rates and decision-making dynamics [8].

Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

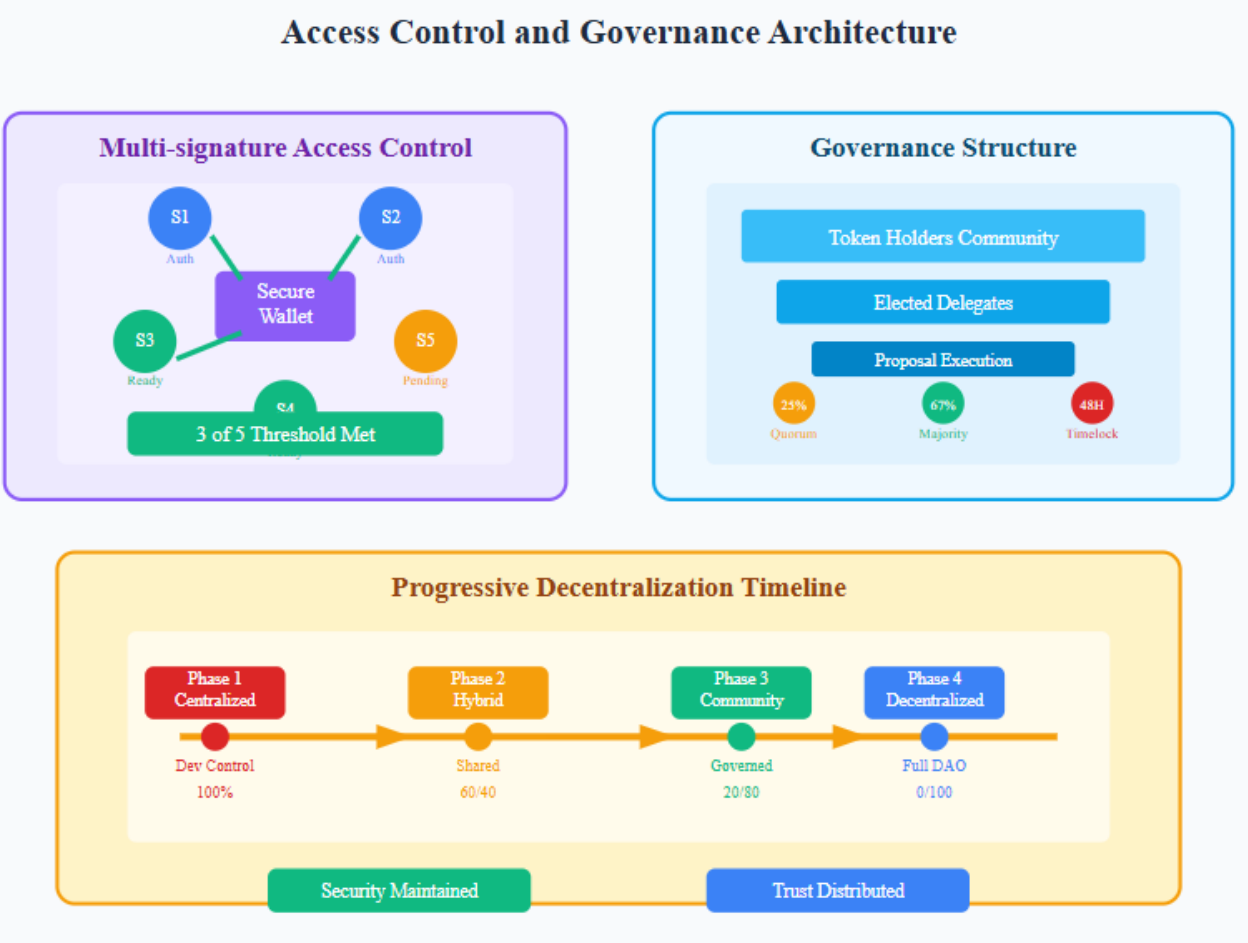

Fig 3. Access Control and Governance Architecture [7, 8].

Financial Protection and Risk Management

Insurance protocols provide crucial financial protection against successful exploits, offering coverage for user funds even when primary security measures fail. These protocols typically involve risk assessment mechanisms that evaluate the security posture of covered protocols and price insurance accordingly. The development of decentralized insurance markets has created sustainable models for protecting DeFi users against protocol failures.

Insurance protocols have emerged as essential components of the DeFi ecosystem, providing financial safeguards that traditional centralized insurance mechanisms cannot offer in decentralized environments. The implementation of decentralized insurance involves sophisticated risk assessment algorithms that analyze smart contract code, audit reports, historical security incidents, and protocol governance structures to determine appropriate coverage terms and premium pricing. Advanced insurance protocols utilize parametric insurance models that automatically trigger payouts when predetermined conditions are met, eliminating the need for traditional claims processing and reducing settlement times. DeFi lending protocols have demonstrated the critical importance of financial protection mechanisms, with lending platforms facilitating billions of dollars in transactions while maintaining complex risk management systems to protect both lenders and borrowers from default risks and market volatility [9].

Treasury management represents another critical aspect of financial security, with protocols maintaining reserve funds to cover potential losses and ensure continued operations. These treasuries should be managed through secure multi-signature mechanisms and invested in low-risk assets to preserve capital while generating sustainable returns. The optimization of treasury management

Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

strategies involves balancing liquidity requirements with yield generation opportunities, ensuring that sufficient funds remain available for emergency situations while maximizing returns on idle capital. Modern treasury management systems incorporate sophisticated portfolio optimization algorithms that dynamically adjust asset allocations based on market conditions, risk assessments, and protocol requirements. DeFi lending and borrowing protocols have evolved to include automated treasury management features that optimize interest rate calculations and collateral requirements based on real-time market conditions and risk assessments [9].

Risk management frameworks help protocols identify and mitigate potential threats before they materialize. These frameworks typically involve continuous monitoring of protocol metrics, regular security assessments, and stress testing under various market conditions. The implementation of comprehensive risk management systems requires integration of multiple data sources, including on-chain transaction data, market price feeds, liquidity metrics, and external threat intelligence. Advanced risk management frameworks utilize machine learning algorithms to detect anomalous patterns and predict potential security incidents before they occur. The effectiveness of risk management systems depends on proper calibration of monitoring parameters and threshold settings that balance sensitivity with false positive rates [9].

The evolution of financial protection mechanisms in DeFi has created complex ecosystems where multiple layers of security work together to protect user funds and protocol integrity. Decentralized finance protocols have fundamentally transformed traditional financial services by enabling direct peer-to-peer transactions without requiring trusted intermediaries, creating new categories of financial risks that require innovative protection mechanisms. The rapid growth of DeFi has been accompanied by significant security challenges, with numerous high-profile incidents resulting in substantial financial losses for protocol users and stakeholders. Analysis of DeFi security incidents reveals patterns of vulnerability exploitation that highlight the critical importance of comprehensive risk management frameworks and financial protection mechanisms [10].

The integration of insurance protocols with broader DeFi ecosystems has created synergistic effects where multiple protection mechanisms work together to provide comprehensive coverage against various types of risks. Modern DeFi protocols implement multi-layered security architectures that combine traditional security measures with innovative financial protection mechanisms, creating resilient systems that can withstand both technical attacks and economic manipulation attempts. The development of standardized risk assessment frameworks has enabled more accurate pricing of insurance products and better allocation of capital across different risk categories [10].

Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

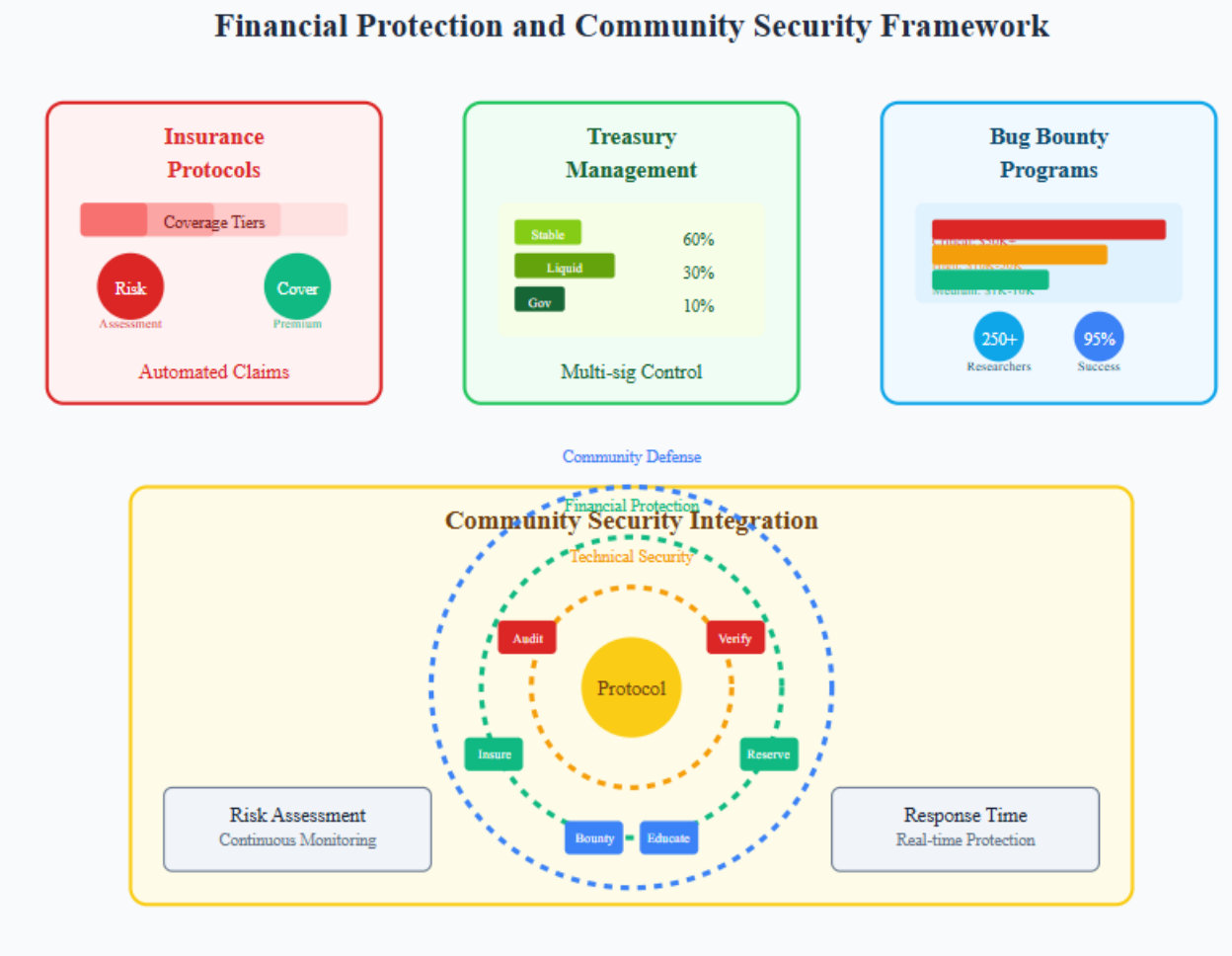

Fig 4. Financial Protection and Community Security Framework [9, 10].

Community-Driven Security Initiatives

Bug bounty programs harness the collective expertise of the security community by providing financial incentives for responsible vulnerability disclosure. These programs should offer competitive rewards that make responsible disclosure more attractive than exploitation, while providing clear guidelines for submission and evaluation processes.

Bug bounty programs have evolved into sophisticated security frameworks that leverage distributed expertise to identify vulnerabilities that traditional auditing processes might overlook. The implementation of effective bug bounty systems requires careful calibration of reward structures to ensure that financial incentives align with responsible disclosure practices rather than malicious exploitation. Advanced bug bounty platforms incorporate multi-tier reward systems that offer different compensation levels based on vulnerability severity, potential impact, and quality of submission documentation. Research demonstrates that blockchain-based bug bounty programs have become essential components of cybersecurity strategies, with the blockchain industry experiencing rapid growth in both the number and sophistication of bug bounty initiatives designed to address unique security challenges in decentralized systems [11].

Community security reviews leverage the distributed expertise of protocol users and developers to identify potential issues that formal auditing might miss. These reviews often focus on economic attack vectors and edge cases that emerge from real-world usage patterns. The effectiveness of community-driven security initiatives depends heavily on the establishment of clear communication channels, standardized review processes, and recognition mechanisms that incentivize high-quality contributions from volunteer security researchers. Modern community security frameworks incorporate collaborative

Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

platforms where multiple researchers can contribute to vulnerability analysis, creating distributed security assessment processes that benefit from diverse perspectives and expertise areas. The blockchain industry has witnessed significant expansion of bug bounty programs, with organizations recognizing the value of crowdsourced security testing in identifying vulnerabilities that internal testing teams might overlook [11].

Educational initiatives within the DeFi community help users understand security best practices and recognize potential threats. Well-informed users serve as an additional layer of defense by avoiding risky behaviors and reporting suspicious activities. The development of comprehensive educational programs requires integration of multiple learning modalities, including interactive tutorials, case study analysis, and hands-on security demonstrations that enable users to understand both theoretical concepts and practical implementation details. Advanced educational frameworks incorporate gamification elements and practical exercises that engage users while teaching essential security concepts. The implementation of bug bounty programs in blockchain environments has revealed unique characteristics that distinguish these initiatives from traditional software security programs, including the need for specialized expertise in cryptographic protocols and smart contract analysis [11].

The evolution of community-driven security initiatives has created ecosystems where distributed expertise can be systematically leveraged to improve protocol security across multiple dimensions. Decentralized finance protocols benefit significantly from community engagement in security processes, as the open-source nature of most DeFi projects enables widespread participation in security assessment and improvement activities. The growth of community-driven security has been facilitated by the development of specialized platforms and tools that enable efficient coordination between security researchers, protocol developers, and user communities. Open source software risk assessment has become increasingly sophisticated, with modern risk scoring methodologies incorporating multiple factors, including code quality, maintainer activity, security vulnerability history, and community engagement levels [12].

The integration of community-driven security initiatives with formal security processes has created hybrid models that combine the rigor of professional security auditing with the distributed expertise and real-world insights of community participants. Modern DeFi protocols implement comprehensive security frameworks that incorporate multiple feedback mechanisms, enabling continuous improvement based on community input and real-world usage patterns. The effectiveness of these integrated approaches depends on proper coordination between different security stakeholders and the establishment of clear communication protocols that ensure important security information reaches relevant decision-makers. Risk scoring frameworks for open source software have evolved to include automated assessment tools that can evaluate security posture across multiple dimensions, enabling organizations to make informed decisions about software adoption and security investment priorities [12].

Conclusion

The comprehensive security architecture proposed in this paper introduces an original, next-generation framework that integrates multiple complementary defense mechanisms across all phases of protocol development and deployment, positioning it as a global benchmark for financial resilience. Pre-deployment security foundations establish robust defensive postures through systematic smart contract auditing, formal verification processes, and transparent code documentation that enables comprehensive community review. Runtime protection mechanisms provide active defense against real-time threats through sophisticated monitoring systems, automated circuit breakers, and rate-limiting controls that prevent exploitation of protocol vulnerabilities. Access control and governance security frameworks ensure distributed authority through multi-signature implementations and progressive decentralization strategies that maintain security while achieving true decentralization. Financial protection and risk management systems create resilient ecosystems capable of withstanding both technical attacks and economic manipulation through insurance protocols, treasury management,

Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

and continuous risk assessment. Community-driven security initiatives harness distributed expertise through bug bounty programs, collaborative security reviews, and educational frameworks that create informed user communities capable of contributing to overall protocol security. The evolution of DeFi security represents a paradigm shift toward distributed, collaborative defense mechanisms that leverage the collective expertise of global security communities while maintaining the decentralized principles fundamental to blockchain technology. Successful implementation of these comprehensive security frameworks requires continuous adaptation to emerging threats, regular updates to protection mechanisms, and ongoing collaboration between protocol developers, security researchers, and user communities to maintain the integrity and trustworthiness of decentralized financial infrastructure.

Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

References

[1] William Peaster, "What is DeFi? Understanding Decentralized Finance," 2021. [Online]. Available: https://www.defipulse.com/blog/what-is-defi
[2] Huaiguang Wu et al., "A Review of Deep Learning-Based Vulnerability Detection Tools for Ethernet Smart Contracts," ScienceDirect, 2024. [Online]. Available: https://www.sciencedirect.com/org/science/article/pii/S1526149224001735
[3] Atefeh Zareh Chahoki and Marco Roveri, "Static Analysis for Detecting Transaction Conflicts in Ethereum Smart Contracts," arXiv, 2025. [Online]. Available: https://www.arxiv.org/pdf/2507.04357
[4] Mandal S, Vishvakarma P, Bhumika K. Developments in emerging topical drug delivery systems for ocular disorders. Current Drug Research Reviews Formerly: Current Drug Abuse Reviews. 2024 Nov 1;16(3):251-67.
[5] Kaihua Qin et al., "Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit," arXiv, 2020. [Online]. Available: https://scispace.com/pdf/attacking-the-defi-ecosystem-with-flash-loans-for-fun-and-3vqvc597fe.pdf
[6] Vishvakarma P, Kumari R, Vanmathi SM, Korni RD, Bhattacharya V, Jesudasan RE, Mandal S. Oral delivery of peptide and protein therapeutics: challenges and strategies. Journal of Experimental Zoology India. 2023 Jul 1;26(2).
[7] Haozhe Zhou et al., "The State of Ethereum Smart Contracts Security: Vulnerabilities, Countermeasures, and Tool Support," MDPI, 2022. [Online]. Available: https://www.mdpi.com/2624-800X/2/2/19
[8] Fabian Schär, "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," ResearchGate, 2021. [Online]. Available: https://www.researchgate.net/publication/350907670_Decentralized_Finance_On_Blockchain-_and_Smart_Contract-Based_Financial_Markets
[9] Garg A, Vishvakarma P, Mandal S. Exploring Carica papaya seeds extract as a herbal jelly for helminthiasis treatment: A comprehensive analysis. World J Pharm Pharm Sci. 2023 Mar 5;12(5):763
[10] Ram Singh, "The Perils of Decentralised Finance (DeFi)," Engage, 2024. [Online]. Available: https://www.epw.in/engage/article/perils-decentralised-finance-defi
[11] Bhatti M, Kumar J, Kareemulla S, Vishvakarma P, Deka P, Singh SP, Pujari NM, Singh S, Dixit CK. Exploring Marine-Derived Bioactive Compounds and Their Impact on Diverse Diseases. Biochemical & Cellular Archives. 2024 Apr 1;24(1).
[12] Viresh Garg, "Open Source Software (OSS) Risk Scoring by OpsMx," OPSMX, 2024. [Online]. Available: https://www.opsmx.com/blog/open-source-software-oss-risk-scoring-by-opsmx/