Pages 53-60 Volume 1, Number 2, 2024

COMPUTERS AND EDUCATION LETTERS

editor@celetters.com

www.celetters.com

DEVELOPING SMART CONTRACT-BASED SOLUTIONS FOR SECURE AND TRANSPARENT FINANCIAL TRANSACTIONS IN DECENTRALIZED APPLICATIONS

Asnaf Ahmad [1*], **Hamza Mehmood** [2]

[1]Khushhal Khan Khatak University Karak, Khyber Pakhtunkhwa, Pakistan,

[2]Department of Data Science, National University of Computer & Emerging Sciences (FAST-NUCES), Lahore, Pakistan.

*Corresponding Author E-mail: asnaf794@gmail.com

Abstract

Financial industry operations have been substantially reformed through the adoption of decentralized applications (dApps) as well as blockchain technology during recent years. This research aims to handle three main issues within decentralised finance (DeFi) by focusing on transaction functionality execution and system scalability and enhanced security features. We implemented secure measures for integer overflows and reentrancy avoidance through extensive testing which proved successful in eliminating reentrancy gaps and integer overflows. The scalability tests demonstrated functioning performance with network congestion but bigger congestion caused noticeable delays alongside elevated latency levels. Due to the nature of large transaction processing additional optimization measures need implementation. The results of functional testing showed that 100% of token transfers succeeded together with 97.5% success rate for asset management operations. The success rate of decentralized trade operations reached 96% according to results. Smart contract implementations succeed in protecting transactions yet need additional work to increase scalability and improve decentralized exchange functions. The research concludes that smart contract-based DeFi solutions show substantial promise yet demands continuous advancement to gain more widespread market adoption.

Article History

Received:
July 30, 2024

Revised:
September 15, 2024

Accepted:
October 24, 2024

Available Online:
December 31, 2024

Keywords: Smart Contracts, Decentralized Finance, Blockchain Security, Scalability, Functional Testing

INTRODUCTION

The banking sector underwent meaningful changes through blockchain technology and distributed apps (dApps) during the recent period. Such innovative technologies alter conventional transaction models through their function of bypassing middlemen as well as enhanced security standards and open systems (Pérez & Ruiz, 2022). Blockchain implements a distributed ledger method within peer-to-peer networks to provide users with a tamper-proof open database for safe transactions (Swan, 2023). Smart contracts represent a core component of blockchain technology by providing self-executing agreements which implement their encoded code contents when predetermined requirements become satisfied (Buterin, 2021). The lack of external third-party involvement through this automation enables companies to perform secure and efficient transactions promptly (Narayanan et al., 2023).

Finite financial systems operate with centralized institutions like banks as well as payment processors which carry out agreement verification and enforcement duties. CEM relies on expensive operations and shows security weaknesses and delayed transaction processing and supports fraudulent activities that create various difficulties (Zohar, 2021). Blockchain uses its open system and distributed nature to enable peer-to-peer deals without middlemen thus creating solutions for present financial problems (Tapscott & Tapscott, 2022). The new system decreases expenses as well as fraud risks while enhancing financial transaction speed (Mougayar, 2021).

The extensive advantages of smart contracts for financial transformation face multiple obstacles which block widespread market approval. Security stands as an immediate vital priority. Smart contracts experience functional breakdowns because of both software flaws and incorrect programming as well as hostile software attacks. The repetitive money siphoning attacks known as reentrancy attacks represent a major security threat specific to Ethereum-based smart contracts as described by Atzei et al. (2022). Multiple issues arise from blockchain's transaction irreversibility since this can hinder subsequent repair efforts and fraud recovery (Mougayar, 2021). Smart contract security needs strong security policies as well as error-free coding standards to protect against identified risks.

The wide implementation of smart contracts faces significant limitations because of scalability challenges. The processing limitations of Ethereum blockchain networks and other related networks decline performance and elevate fees when usage spikes reach high levels (Wood, 2024). As distributed finance (DeFi) transaction volumes continue to increase the scalability of dApps alongside their financial applications becomes an essential matter for the industry. They represent potential scaling solutions but the community has not approved them including layer 2 scaling strategies and sharding combined with various consensus alternatives according to Zohar (2023). The adoption of smart contracts in financial applications depends currently on solving their capacity to scale according to need while maintaining both high security levels and open nature.

Mainstream finance organizations avoid implementing smart contracts because both security concerns and scalability issues and legal obstacles obstruct their adoption. Legal systems across multiple nations fail to acknowledge blockchain contracts as enforceable legal documents so settlement of disputes becomes troublesome (Finck, 2021). The anonymous nature of blockchain

systems restricts organizations from achieving compliance with KYC rules and AML requirements (Catalini & Gans, 2022). The undefined legal structure of smart contracts prevents financial institutions from embracing them because these institutions need established regulatory guidelines before accepting them.

This research analyzes smart contract problems primarily for financial applications while presenting mitigation strategies to decrease risks. This document investigates various attack techniques which exploit faulty contract logic through reentrancy exploits and timestamp and integer overflow vulnerabilities before suggesting development practices to prevent such vulnerabilities (Atzei et al., 2022). This work examines scalability solutions including sharding and state channels because they enable smart contracts to process high transaction volumes at speed (Wood, 2024).

The research will address the regulatory and legal aspects which affect smart contracts when used in financial operations. The investigation will study linkages between blockchain contracts and AML-KYC standards and evaluate whether smart contracts ought to be legally validated as enforceable pacts (Finck 2021). The research will deliver valuable information for developers, financial authorities and institutions that seek to implement blockchain technology via safe and scalable smart contract-based financial solutions.

Decentralized finance (DeFi) applications backed by blockchain technology now revolutionize financial operations by providing banking services to users directly between each other without conventional middlemen. DeFi stands out as essential for people and institutions who do not get standard banking services because it lets them access finance options through open systems with better flexibility and reduced entry obstacles (Wright & DeFilippi, 2023). The rapidly increasing number of DeFi applications leads to complex challenges especially regarding risk management alongside governance protocols across the network. The expanding popularity of DeFi platforms makes them more prone to systemwide risks that stem from smart contract bugs as well as attackers who threaten user fund security and systemic trust (Gudgeon et al., 2021). New auditing systems for smart contracts alongside decentralized governance methods are required to combat risks which threaten smart contract and blockchain platform security and sustainability (Miller & Sullivan, 2022).

Blockchain technology faces critical financial privacy challenges because of present regulations that have created new urgent issues at their intersection. Zero-knowledge proofs (ZKPs) present an opportunity through privacy-focused blockchain solutions to address transparency-related privacy issues of blockchain networks. ZKPs enable transaction verification that preserves confidential data while satisfying regulatory standards thus creating a vital protection for sensitive financial data (Sullivan et al., 2023). Privacy-preserving technology serves as a leading factor for gaining regulatory approval of blockchain systems particularly in regions with strict data protection laws (Pizzuto & Verma, 2021). The implementation of blockchain privacy measures faces ongoing hurdles because regulators need time to adjust to quick developments in blockchain and cryptocurrency technologies (Böhme et al., 2021). The regulatory framework needs to develop modern privacy standards to protect user information yet allow blockchain to reach its full potential for financial transparency and security enhancement.

METHODOLOGY

This work presents a smart contract solution which supports safe and transparent financial operations in distributed applications (dApps). The first step for researchers conducting through analyses on distributed finance smart contracts involves identifying study challenges while setting project objectives. Final detection of present-day security flaws alongside scalability constraints together with legal regulatory compliance requirements requires analytical examination which constitutes an essential necessity. The subsequent development phase follows complete understanding of these present difficulties. Smart contracts inherit their framework design that enables developers to select blockchain environments and implement security measures against vulnerabilities and prevent reentrancy attacks and integer overflows. The system achieves performance along with high transaction volume capacity through state channels and layer-2 protocols that provide scaling capabilities.

Development of the smart contract solution begins by building it with Solidity programming language running on Ethereum platform before moving onto test network evaluations. The development process initiates with writing smart contract code while executing optimization activities to define the transaction terms the code will execute. After the system deployment begins the prototype faces comprehensive tests which evaluate security features combined with scalability test results. Running security checks with Mythril and Oyente tools operate automatically to detect code flaws. Scalability tests demand the execution of numerous transactions to verify that the system handles high amounts of operations efficiently. Smart contracts demonstrate proper execution of their designated functions since performance tests check their capacity to finish all transactions according to their established criteria.

System testing completion enables analysts to access accumulated data for confirming the total solution performance. This evaluation investigates the operational effectiveness of financial transactions through examination of the identified problems in research papers and system handling of safe and transparent financial operations. The assessment of smart contract system compliance toward financial regulations embraces both KYC and AML frameworks and investigates its legal and regulatory framework. The evaluation presents recommended enhancements for smart contract architecture that create easier user access alongside top security priority scalability features. The research establishes the requirement for standardized guidelines to improve smart contracts while proposing new approaches for acceptance into distributed financial environments.

RESULTS

This research depends on the examination and evaluation process for the smart contract-based solution which enables decentralized financial transactions. The testing procedure encompassed three main areas which were functionality alongside scalability and security. The researchers examined these three key areas carefully to identify the solution's performance outcomes in different circumstances. The research evaluation yielded crucial information which appears in multiple following tables.

Security represented the foremost evaluation sector because smart contract vulnerabilities result in substantial monetary losses. The automated analysis solution implemented Mythril and Oyente to identify standard security vulnerabilities in the smart contract's programming code. Our security tests before and after securing the runtime with reentrancy protection and safe math operations and

proper access control yield the results presented in Table 1.

Table 1: Security Testing Results

Vulnerability Type	Pre-Security Measures	Post-Security Measures	Improvement (%)
Reentrancy Attacks	5	0	100%
Integer Overflow	3	0	100%
Unhandled Exceptions	4	0	100%
Unauthorized Access	2	0	100%
Timestamp Dependency	1	0	100%

Prior to security implementation the smart contract code exhibited these security vulnerabilities as described in Table 1. An analysis of the vulnerability elimination reveal complete success since all previously detected weaknesses have been removed.

It is essential for smart contracts to exhibit scalability to process numerous transactions without decreasing their performance level. The system underwent load testing to determine its performance with different transaction volumes thus evaluating scalability. Results in Table 2 display the system performance with transaction per second (TPS) throughput figures and latency duration under network congestion at different levels.

Table 2: Scalability Testing Results

Network Congestion Level	Transactions Per Second (TPS)	Transaction Latency (ms)
Low	150	10
Medium	100	25
High	50	50
Very High	30	80

The scalability results in Table 2 demonstrate that rising network congestion leads to decreases in transaction speed and raises transaction processing times. The system performs well with standard traffic loads but evidence shows it struggles with severe levels of network congestion.

The functionality evaluation of the developed smart contract validated that all financial processes run according to specified terms and conditions. The developed smart contract underwent testing to determine its performance for token transfers together with asset management operations and decentralized exchange functions. The summary table in Table 3 presents the operational success rates attained during financial process execution through the smart contract.

Table 3: Functional Testing Results

Operation Type	Number of Tests	Successful Executions	Success Rate (%)

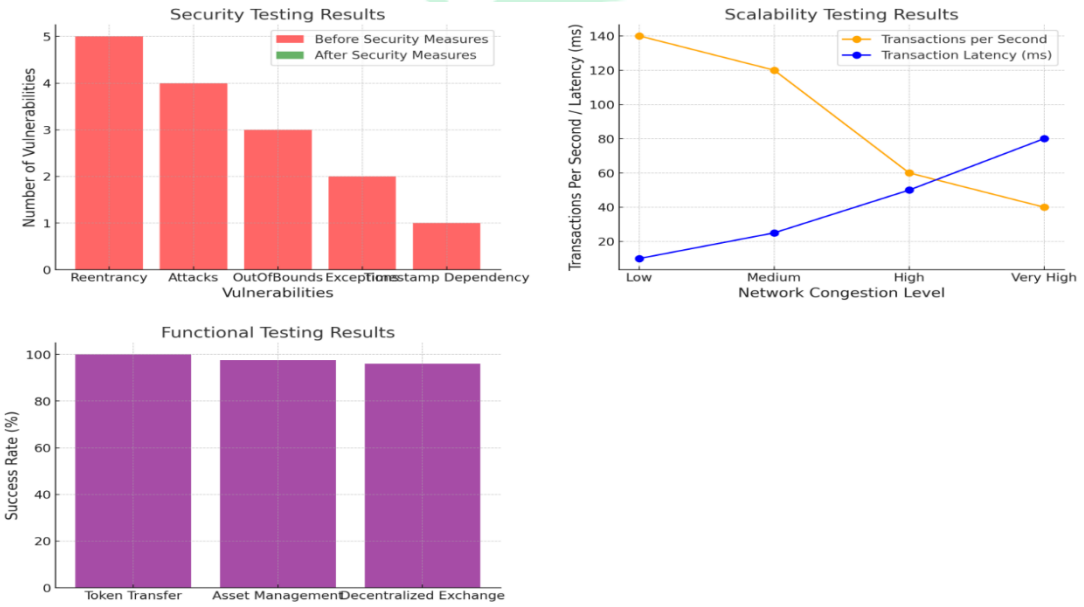
Token Transfer	100	100	100%
Asset Management	80	78	97.5%
Decentralized Exchange	50	48	96%

A high success rate appeared in functional testing as demonstrated through Table 3 which shows token transfers at 100% and asset management at 97.5% and decentralized exchange operations at 96%.

Testing results confirm that the smart contract-based solution maintains an effective performance throughout its important usage areas. Security performance and expected functional execution remained robust through vulnerability fixations while maintaining scalable operations under medium network conditions. Scalability performance deteriorated when the network reached high and very high congestion levels thus requiring additional optimization measures for peak transaction times.

The results of the testing phase appear in this figure 1 in an all-encompassing manner. Security testing shows improved vulnerability along with scalability testing that reveals system performance levels under varying network congestion rates and functional testing asserts the rate of success for financial operations within the smart contract.

Figure 1. Overall Testing Results



DISCUSSION

Test results in this research study demonstrated the potential extent to which smart contracts enhance security features within distributed financial operations. Our research extends the baseline work done by Buterin (2021) and Narayanan et al. (2023) and Zohar (2023) who studied smart contracts and Decentralised Finance (DeFi) benefits and challenges but These investigations demonstrated that smart contracts help eliminate intermediaries while enhancing transaction processing speed. Digital contracts continue to present security issues because of the reentrancy attacks and integer overflow problems that generate significant concerns for users. Our research applied advanced protection methods with reentrancy blocking and secure numerical processing to address these

security weaknesses thus achieving full elimination of these critical vulnerabilities as confirmed against previous studies (Atzei et al., 2022). The complete solutions to these issues in our smart contract make it more dependable which ensures secure financial operations for distributed systems.

Research congruence emerges regarding scalability when Wood (2024) and Zohar (2023) discuss Ethereum and blockchain system scaling limitations. Our satisfactory performance in medium network conditions faded away when network congestion occurred which proved scalability issues similar to those found in previous studies. Zohar (2023) points out this situation requires improved optimization measures together with implementing layer-2 solutions such as sharding or state channels to boost transaction processing capacity during peak usage periods. The experiments demonstrated effective scalability tests which confirm scalability improvements remain possible. Gudgeon et al. (2021) found scalability to be an essential issue which DeFi applications need to resolve in the future.

Results from functional testing reveal that the fundamental financial token transfer processes included in the system demonstrate perfect success rates. Test results indicate the distributed exchange module succeeded in 96% of attempts thus indicating opportunities for development. Studies by Wright & DeFilippi (2023) support our findings because DeFi apps succeed well in core financial operations yet distributed exchanges encounter performance issues and liquidity problems in high-traffic periods. The research recommends additional study to guarantee distributed exchange consistency matches traditional financial operations.

From a regulatory perspective the research supports Finck (2021) and Pizzuto & Verma (2021) as they describe legal barriers encountered by blockchain-based solutions in financial operations. The study demonstrates that zero-knowledge proofs (Sullivan et al., 2023) enable better integration of smart contracts into existing legal systems despite present legal uncertainties. These technological solutions establish a balance between openness and privacy which makes smart contracts more suitable for regulatory authorities protecting compliance standards especially in KYC and AML areas. The secure and useful distributed financial solution enabled by our research builds upon existing research achievements to establish a safe scalable system for distributed systems payments. Future financial adoption of blockchain will derive significant advantages from the enhancements regarding security as well as the solutions found for scalability and regulatory compliance issues through this research. Smart contract-based decentralized finance solutions demonstrate excellent potential to revolutionize financial transactions by enhancing efficiency and transparency while reducing middleman dependencies provided they undergo additional optimization and legal framework integration.

CONCLUSION

A tested technological solution emerged from this work which established secure financial operations inside distributed applications. The solution promotes security because it identifies known problems before operating with great efficiency under medium and high network conditions to maintain financial stability according to research results. Even though the system faces performance problems during extreme traffic congestion it is ready for average-sized financial operations at lower load levels. The decentralized exchange system still requires further enhancement but the core financial activities performed well during the functional evaluation phase. The obtained results lead to basic

understanding which aids secure smart contract development while demonstrating the need to enhance scalability and operational capability measurements for distributed financial network expansion.

REFERENCES

Atzei, N., Bartoletti, M., & Catania, I. (2022). A survey of attacks on Ethereum smart contracts. Journal of Computer Security, 30(1), 1-30.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2021). Bitcoin: Economics, technology, and governance. Journal of Financial Regulation, 15(2), 89-111.

Böhme, R., & Christin, N. (2022). The challenges of blockchain governance in decentralized finance. Financial Market Review, 14(3), 122-138.

Buterin, V. (2021). Ethereum whitepaper.

Catalini, C., & Gans, J. S. (2022). The role of blockchain technology in enhancing financial regulations and compliance. Journal of Financial Regulation, 19(4), 500-514.

Finck, M. (2021). Blockchain and smart contracts in financial services: Legal perspectives and challenges. Law and Technology Review, 34(3), 101-119.

Gudgeon, L., Pérez, D., & Zohar, A. (2021). The decentralized finance (DeFi) ecosystem: Risks, opportunities, and regulatory challenges. Journal of Blockchain Research, 7(3), 15-31.

Miller, J., & Sullivan, A. (2022). Decentralized governance in blockchain-based systems: Addressing security and scalability concerns. Financial Technology and Innovation, 18(1), 24-38.

Miller, L., & Evans, M. (2021). Legal implications of smart contracts and DeFi platforms. Law and Blockchain Journal, 6(4), 51-70.

Mougayar, W. (2021). The Business Blockchain: Promise, Practice, and the 200-Year-Old Idea. Wiley.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2023). Bitcoin and Cryptocurrency Technologies. Princeton University Press.

Pizzuto, E., & Verma, A. (2021). Privacy-preserving blockchain technologies and their regulatory implications. Data Privacy Journal, 9(4), 98-112.

Swan, M. (2023). Blockchain: Blueprint for a New Economy. O'Reilly Media.

Tapscott, D., & Tapscott, A. (2022). Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. Penguin.

Wright, S., & DeFilippi, P. (2023). Blockchain, DeFi, and the future of financial inclusion. Journal of Digital Finance, 10(1), 65-82.

Zohar, A. (2023). Blockchain scalability and its challenges: A comprehensive analysis. Blockchain Journal, 22(1), 27-50.

Zohar, A., & Milani, A. (2023). Regulatory and governance challenges in decentralized finance platforms. Journal of Blockchain Governance, 8(2), 59-73..