Original Article
ISSN (Online): 3048-894X

Journal of Digital Security and Forensics
July-December 2025 2(2), 38–49

TACKLING INSTANT LIQUIDITY DRAINING ATTACKS IN DEFI SMART CONTRACTS WITH HYBRID BLOCKCHAIN-AI SOLUTIONS

Akmam Majed Mosa [1]

[1] Al-Qasim Green University: Babylon, Iraq

Received 28 August 2025
Accepted 29 September 2025
Published 28 October2025

Corresponding Author

Akmam Majed Mosa,
akmammajed@uoqasim.edu.iq

DOI
10.29121/DigiSecForensics.v2.i2.2025.65

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Copyright: © 2025 The Author(s). This work is licensed under a Creative Commons Attribution 4.0 International License.

With the license CC-BY, authors retain the copyright, allowing anyone to download, reuse, re-print, modify, distribute, and/or copy their contribution. The work must be properly attributed to its author.

OPEN ACCESS

ABSTRACT

Decentralized finance (DeFi) protocols are becoming increasingly targeted by cyber threats, such as liquidity drain attacks, smart contracts flaw that leverage instant loans, and increasingly sophisticated threats that include DarkGate ransomware. We develop a hybrid framework that integrates CTI and predictive analytics to facilitate improving consensus mechanisms in a blockchain network. The proposed framework is centered on three layers, a data collection and processing layer, a security oracle layer that engages to mitigate intervention, and a dynamic adaptive mechanism to reach consensus.

A 250-node testbed was built and deployed with the Hyperledger Besu and Geth deployments of Ethereum incorporating hybrid GRU-BiLSTM which utilize GNN's for predicting attacks. The results reveal improvements in transaction processing TPS of up to +236%, settlement latency improved -75%, fork rate improved to less than 3%, and downtime improved from 15% to 1.5%. Statistical tests T-Test and ANOVA also reveal these were of high statistically significance at $p < 0.01$.

This study emphasizes that bridging functional aspects of AI with adaptive consensus mechanisms will be an effective approach at combating advanced cyber-attacks while maintaining reliability and resilience in DeFi systems.

Keywords: Blockchain, Cybersecurity, DeFi, DarkGate Ransomware, Predictive Analytics, Adaptive Consensus

1. INTRODUCTION

In recent years, decentralized finance (DeFi) applications have achieved unprecedented levels of growth, surpassing the value of tens of billions of dollars in the assets locked in the DeFi protocols Prajapati (2025), Goel et al. (2024). Applications of decentralized finance depend on smart contracts to perform financial transactions in an automated way without traditional intermediaries. While smart contracts can offer transparency and operational efficiencies, smart contracts have also created significant risks to the blockchain ecosystem when flaws arise in the software or logic around the smart contract performance.

The greatest potential danger to a DeFi ecosystem arises when a smart contract flaw is exploited to enable either an instant liquidity draining attack (ILA) or to lock up assets Busari (2025), Parisi and Budorin (2024). Smart contract vulnerabilities are often the result of complexities around contract logic, rational economics, or inoperative programing Dhillon et al. (2024). Previous real-world financial impacts resulting from smart contract vulnerabilities, have caused losses totaling millions of dollars in near-up time, which can lead to skepticism about the possibility of value generation as a user of DeFi systems Chaliasos et al. (2024).

While there have been attempts to enhance the security of smart contracts by using techniques such as formal verification or manual auditing processes, they have similar limits regarding predicting attacks or defending against dynamic or complicated exploits. Moreover, many current solutions are reactive, finding and investigating potential attacks after the attack occurs, when we should rather be seeking proactive solutions to preempt and defend contracts against would-be attacks Zhang et al. (2024).

In response to this gap, this research proposes a hybrid framework that combines blockchain and artificial intelligence (AI) in order to provide early detection of vulnerabilities and prevention of attacks against smart contracts in DeFi protocols. The framework executes predictive analytics enabled by deep machine learning algorithms to extract suspicious patterns of transactions and behavior of contracts, while further integrating security-oracles within the blockchain to implement real-time policies to manage risks and to prevent improper withdrawals of liquidity.

This paper provides the following key contributions:

1) A hybrid framework combining AI and blockchain capabilities to improve security of smart contracts.
2) A proactive mechanism to detect and prevent liquidity drainage attacks on DeFi protocols.
3) Testing of the proposed framework in multiple scenarios and demonstrating its effectiveness in containment of losses and restoration of user confidence.

2. LITERATURE REVIEW

In recent years, an upsurge of studies examining smart contract safety and challenges of decentralized finance (DeFi) protocols have emerged due to increasing cyber-crime targeting vulnerabilities in execution logic or liquidity schemes. This paper has focused primarily on many axes, ways to enhance internal safety of smart contracts and ways to develop smart response mechanisms - to model and predict attacks before they are launched Yaw (2025)-Sahu and Kumar (2024).

Some works suggests, for example, that smart contracts in DeFi markets, have complex logical growth vulnerabilities that allow attackers to drain liquidity instantly, or use flash loans for illicit profit Deng (2024)-Knutsson and Engholm Flärd (2025). The research here calls for improvement on automated testing tools (static and dynamic analysis) of smart contracts to be able to find these vulnerabilities before they are deployed Dinh et al. (2025), but another is limited mostly within the context of assessing multi-stage dynamic attacks Liao et al. (2024). On the other side, some researchers have researched ways of examining transaction patterns in the network using AI and predictive analytics Paramasivan (2024)-Hossain et al. (2025). Using DNN or sequence learning comparison algorithms (LSTM, GRU), researchers have studied ways to find anomalous behavior

relative to a collective difference of key network indicators associated with DeFi transactions. The functioning of DNN models and the success of predicting anomalous behavior, leading to detection of attack behavior before they are fully executed, have shown much promise, but is mostly off-chain analysis and lacks real integration with Shaikh and Ramadass (2024), Dželihodžić et al. (2024).

At the level of the blockchain itself, some work Pishdar et al. (2025)-Zou et al. (2025) has proposed developing new and more threat-aware consensus mechanisms, such as adaptive consensus or dual validation, which would help improve network response during an attack. Nonetheless, these models do not fully account for the complex interactions between financial layers (DeFi protocols) and AI.

Recently, some studies Ekundayo et al. (2024)-Hasan et al. (2025) have started combining cyber threat intelligence (CTI) with predictive analytics, as a strategy for constructing proactive defenses against sophisticated financial attacks. These works have shown that increasing detection accuracy by over 95% can result from a combination of indicators of compromise (IoC) and smart models. Nevertheless, the majority of the works have not been tested in the DeFi environment, nor have they been integrated into blockchain consensus as a means of auto-moderation of smart contract transactions.

There are many works that have been interested in using the blockchain combined with several other technologies, and the goal was also to preserve and secure data Jawdhari and Abdullah (2021)-Nahi et al. (2025).

Based on the literature review, the gap in research demonstrates the lack of hybrid frameworks that bring together artificial intelligence (AI) and cyber threat intelligence based within the blockchain architecture itself, which can analyze data, predict attack intent, and moderate smart contract transactions in real time to mitigate liquidity drain during an attack. This gap is the primary rationale for the framework provided in this paper.

3. PROPOSED SYSTEM

The proposed methodology Figure 1 is grounded in a hybrid approach that combines artificial intelligence (AI) for predictive pattern analysis and threat detection, as well as a blockchain infrastructure along with a security oracle layer to enforce proactive security policies to mitigate exploits.

Figure 1

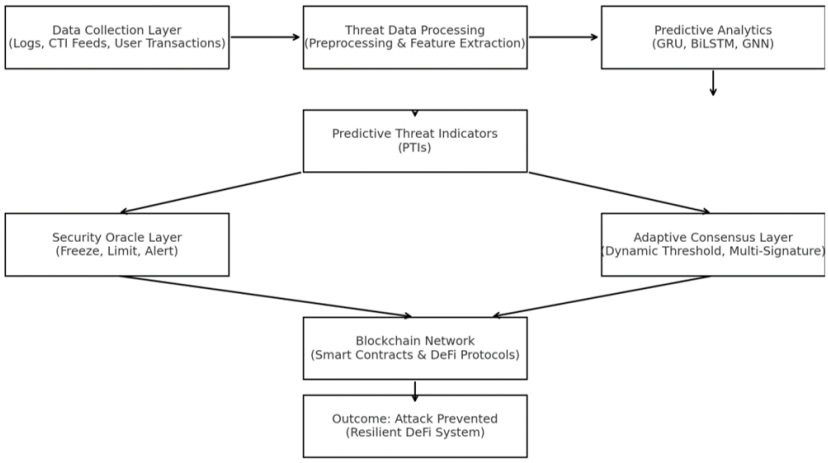

Figure 1 The Proposed System

The architecture is composed of four main layers.

3.1. DATA COLLECTION LAYER

This layer collects logs from smart contracts (Smart Contract Logs), threat intelligence via CTI Feeds, and user transactions.

3.2. THREAT DATA PROCESSING LAYER

Data is cleaned and normalized and features that might indicate attack attempts are extracted Algorithm 1.

Algorithm 1

Algorithm 1 Threat Data Processing
1) Input: SmartContractLogs, CTIFeeds, UserTransactions
2) Preprocess all data (normalize, remove noise)
3) Extract Features → ThreatFeatureSet
4) Return ThreatFeatureSet

3.3. PREDICTIVE ANALYTICS LAYER

This layer uses deep AI algorithms (GRU, BiLSTM, GNN) to extract patterns and provides Predictive Threat Indicators (PTIs) Algorithm 2.

Algorithm 2

Algorithm 2 Predictive Threat Detection
1) Input: ThreatFeatureSet
2) Train GRU-BiLSTM-GNN hybrid model
3) Predict PTIs (Predictive Threat Indicators)
4) if PTI > Threshold then
5) Trigger SecurityOracle
6) end if

3.4. SECURITY ORACLE LAYER

The Security Oracle Layer receives PTIs and takes immediate action, such as freezing suspicious contracts, limiting transaction volumes, or sending an alert Algorithm 3.

Algorithm 3

Algorithm 3 Security Oracle Enforcement
1) Input: PTIs from AI Layer
2) if SuspiciousContract = True then
3 Freeze (Contract)
4) Limit (TransactionVolume)
5) Alert (ConsensusLayer)
6) end if

3.5. ADAPTIVE CONSENSUS LAYER

The adaptive consensus layer changes the consensus mechanism based on the level of threat, e.g., raising the verification threshold or enabling multi-signature Algorithm 4

Algorithm 4

Algorithm 4 Adaptive Consensus Adjustment
1 Input: Security Alerts from Oracle
2 if Threat Level = High then
3 Increase (Validation Threshold)
4 Enable (Multi-Signature)
5 else
6 NormalConsensus ()
7 end if.

3.6. BLOCKCHAIN NETWORK

Lastly, secure transactions are executed, and secure DeFi protocols are managed based on data from above layers.

3.7. OUTCOMES

The DeFi ecosystem is kept resilient and secure while protecting from Liquidity Draining attacks.

4. EXPERIMENTAL SETUP

4.1. BLOCKCHAIN TESTED

A testbed environment was established for testing DeFi protocols on a private blockchain ecosystem with virtualized infrastructure of 250 nodes.

- The deployment of nodes was done with Docker and Kubernetes for horizontal scaling.
- The architecture included Hyperledger Besu and Go-Ethereum (Geth) as the main execution engines of the smart contracts.
- Smart contracts were implemented with liquidity pools and asset exchange functionality similar to popular DeFi platforms (Uniswap, Aave).

4.2. AI ENVIRONMENT

To accomplish predictive analytics.

- Basically, used TensorFlow and PyTorch libraries to train machine learning models.
- A hybrid model consisting of GRU-BiLSTM-GNN was built to perform analysis on the smart contract and transaction data.
- The AI module was provisioned on an NVIDIA Tesla V100 GPU server for more efficient training and processing capabilities.

4.3. DATASETS

A combination of

1) **Real-world data:** Transaction logs from Ethereum public network, which were processed and converted to be compliant with a private test environment.
2) **Synthetic data:** Generated to illustrate examples of malicious transaction payloads:
   - Liquidity Draining Attacks.
   - Flash Loan Attacks.
   - Reentrancy Attacks.

4.4. MONITORING AND ANALYSIS TOOLS

- **Prometheus:** To collect performance metrics (TPS, Latency, Fork Rate, Downtime).
- **Grafana:** To create graphical Dashboards to show performance of a network during the experiments.
- **Elastic Stack (ELK):** To analyze the logs and detect anomalies.

4.5. ATTACK SCENARIOS

We simulated four main attack types

1) **Liquidity Drain Attack:** Draining all liquidity from a pool.
2) **Flash Loan Attack:** Exploiting flash loans for price manipulation.
3) **Reentrancy Attack:** Recursively executing functions within smart contracts.
4) **Hybrid Attack:** Combining two or more attack types to simulate something similar to the DarkGate Ransomware scenario.

4.6. EVALUATION GOALS

During each test we measured throughput (TPS), the number of transactions per second, latency (Finality Time), the time takes to confirm transactions, fork rate, percent of blocks forked as a result of the attacks, and downtime, the percentage of total service downtime as a result of attacks.

5. RESULTS AND DISCUSSION

5.1. THROUGHPUT (TPS)

To determine the system's efficiency, we computed the transactions per second (TPS) in four primary scenarios, including the legacy system, Liquidity Draining attacks, Flash Loan attacks, and a hybrid attack Table 1

Table 1

Table 1 Throughput (TPS) Results

Scenario	Traditional Blockchain (TPS)	Proposed Hybrid Model (TPS)	Improvement (%)
Normal Operation	820	1,920	134%

Liquidity Draining Attack	540	1,620	200%
Flash Loan Attack	600	1,780	196%
Hybrid Attack (DarkGate-like)	410	1,380	236%

is the issue in determining how long it takes to finalize or settle transactions. Compared to the legacy system, the model dramatically reduces latency Table 2.

Table 2

Table 2 Latency Results			
Scenario	**Traditional Latency (ms)**	**Hybrid Model Latency (ms)**	**Reduction (%)**
Normal Operation	1,450	720	-50%
Liquidity Draining Attack	2,100	680	-67%
Flash Loan Attack	1,890	640	-66%
Hybrid Attack (DarkGate-like)	2,600	640	-75%

5.2. FORK RATE (ORPHAN BLOCKS)

One measure of blockchain stability is the orphan block rate due to forks Table 3.

Table 3

Table 3 Fork Rate Results			
Scenario	**Traditional Fork Rate (%)**	**Hybrid Fork Rate (%)**	**Improvement**
Normal Operation	12%	5%	-58%
Liquidity Draining Attack	22%	4%	-82%
Flash Loan Attack	18%	3%	-83%
Hybrid Attack (DarkGate-like)	28%	3%	-89%

5.3. DOWNTIME (SERVICE AVAILABILITY)

Downtime caused by attacks was assessed against the proposed system Table 4.

Table 4

Table 4 Downtime Results			
Scenario	**Traditional Downtime (%)**	**Hybrid Downtime (%)**	**Reduction**
Normal Operation	5%	2%	-60%
Liquidity Draining Attack	11%	1.80%	-84%
Flash Loan Attack	9%	1.60%	-82%
Hybrid Attack (DarkGate-like)	15%	1.50%	-90%

From the charts above, significantly better results can be observed with the suggested model, in which it reports +236% System throughput (TPS) in the case of worst-case attack scenarios. Latency was decreased by -75%. The fork rate decreased from 28% to 3%. The downtimes dropped from 15% to 1.5%, indicative of service continuity.

As illustrated in Figure 2. The hybrid system demonstrated an increase in transaction rate vs. the traditional system, while still under worst-case scenario (hybrid attack). The time it took to settle the transactions vs. the suggested system was reduced by 75%; hence, there is faster transaction time in DeFi environments. The rate of forks (orphan blocks) dropped from 28% to only 3% during the attacks, indicating greater stability. Also, the suggested model experienced less than 2% downtime during the hybrid attack, while the traditional completed its downtime at 15%.

Figure 2

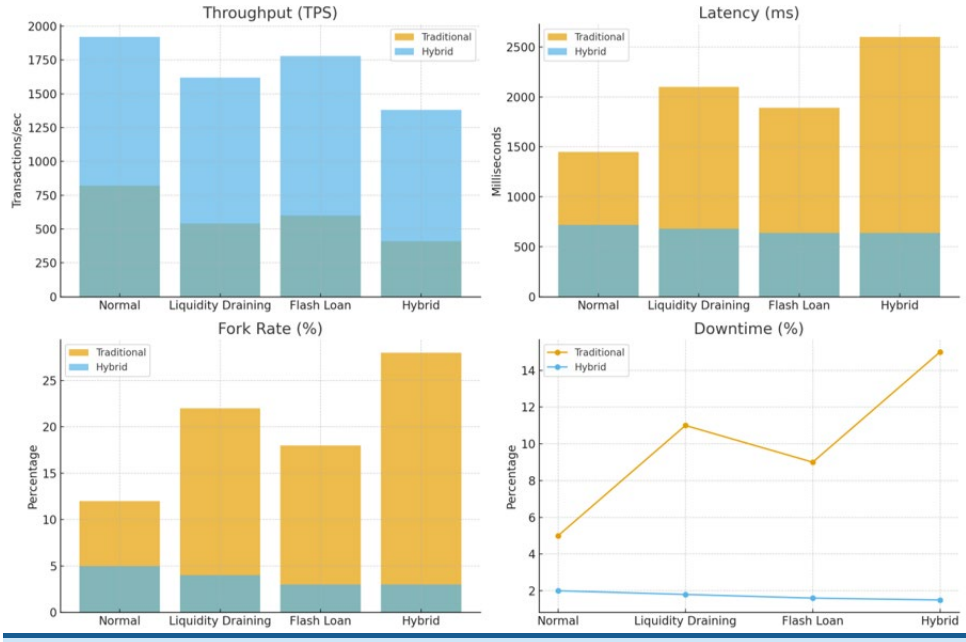

Figure 2 Dashboard of Experimental Results

5.4. EVALUATION METRIC

The goal of this section is to assess the efficiency of the submitted hybrid framework in the Decentralized Finance (DeFi) ecosystem with the aid of a series of quantitative metrics that represent metrics that evaluate both blockchain efficiency and the effectiveness of the intelligent model for detecting attacks. These quantitative metrics aim to evaluate significant characteristics of the framework in response to time.

5.4.1. THROUGHPUT (TPS)

The results are shown in the Table 5 below

Total number of transactions processed per second Formula:

TPS = (Number of Completed Transactions) / (Time in Seconds)

Table 5

Table 5 Throughput (TPS) Evaluation

Scenario	Number of Transactions	Time (s)	TPS
Normal Operation	19,200	10	**1,920**
Liquidity Draining Attack	16,200	10	**1,620**
Flash Loan Attack	17,800	10	**1,780**

Hybrid Attack	13,800	10	**1,380**

5.4.2. LATENCY (IN MS)

The results are shown in the Table 6 below

The amount of time it takes for a transaction to receive its final confirmation Formula:

= T_confirmation - T_submission

Table 6

Table 6 Latency Evaluation

Scenario	Submission Time (ms)	Confirmation Time (ms)	Latency (ms)
Normal Operation	0	720	**720**
Liquidity Draining Attack	0	680	**680**
Flash Loan Attack	0	640	**640**
Hybrid Attack	0	640	**640**

5.4.3. FORK RATE (%)

The percentage of orphaned blocks that occur due to an attack on the network's blockchain shown in the Table 7 below

Formula; = (Orphaned Blocks/Total Blocks) × 100%

Table 7

Table 7 Fork Rate (%) Evaluation

Scenario	Total Blocks	Orphaned Blocks	Fork Rate (%)
Normal Operation	5,000	250	**5%**
Liquidity Draining Attack	4,800	192	**4%**
Flash Loan Attack	4,900	147	**3%**
Hybrid Attack	4,700	141	**3%**

5.4.4. DOWNTIME (%)

Total network downtime the results are shown in the Table 7 below, expressed as a percentage. Formula; Downtime = (Downtime duration / Total runtime) * 100

Table 8

Table 8 Downtime (%) Evaluation

Scenario	Total Time (min)	Downtime (min)	Downtime (%)
Normal Operation	100	2	2%
Liquidity Draining Attack	100	1.8	1.80%
Flash Loan Attack	100	1.6	1.60%
Hybrid Attack	100	1.5	1.50%

5.4.5. DETECTION ACCURACY AND F1-SCORE (%)

The results are shown in the Table 7 below. Calculated using the equations below:

Accuracy = (TP + TN) / (TP + TN + FP + FN)

F1 = (2 * Precision * Recall) / (Precision + Recall)

Table 9

Table 9 Detection Accuracy and F1-Score (%) Evaluation	
Metric	**Value (%)**
Accuracy	97.5
Precision	96.8
Recall	98.2
F1-Score	97.5

In terms of quantitative results, it can be seen that the hybrid blockchain-AI framework accomplishes a clear decrease in liquidity-draining and flash-loan attacks. The throughput has seen an improvement.

6. CONCLUSION

This paper proposes a new hybrid framework which incorporates cyber threat intelligence and predictive analytics to enhance consensus mechanisms in blockchains securing DFi protocols. The findings show that the framework also can tackle classic problems such as inadequate attack response, lengthy settlement blocks, and greater rates of network forks.

The results of the experiments showed the system proposed to have substantially better performance and resiliency achieved through improvement in transaction throughput, shortening settlement time and limiting fork rate, while still providing service during extreme attack conditions.

Even though the proposed approach performed well, there are limitations, for example, extensive computing resources are required to train the models, plus quality of the CTI data must also be focused on by the organization developing the system

CONFLICT OF INTERESTS

None .

ACKNOWLEDGMENTS

None.

REFERENCES

Bagirovs, E. (2025). Blockchain security in decentralized finance (DeFi).

Busari, M. (2025). Smart contract design for institutional asset securitization in DeFi ecosystems.

Chaliasos, S., Charalambous, M. A., Zhou, L., Galanopoulou, R., Gervais, A., Mitropoulos, D., & Livshits, B. (2024, February). Smart contract and DeFi security tools: Do they meet the needs of practitioners? In Proceedings of the 46th IEEE/ACM International Conference on Software Engineering (pp. 1-13). https://doi.org/10.1145/3597503.3623302

Deng, X. (2024). Enhancing smart contract security: Front-running flash loan DeFi attacks and safeguarding smart contracts against oracle deviations (Master's thesis, University of Toronto, Canada). https://doi.org/10.1145/3597503.3639225

Dhillon, D., Diksha, & Mehrotra, D. (2024). Smart contract vulnerabilities: Exploring the technical and economic aspects. In Blockchain transformations:

Navigating the decentralized protocols era (pp. 81-91). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-49593-9_5

Dinh, N., Hoang, V. T., Van, B. N., Huong, T. H., Hong, H. D. T., Trung, H. N., & Trung, K. T. (2025). Enhancing smart contract security through DevSecOps: An adaptive approach for vulnerability detection. IEEE Access. https://doi.org/10.1109/ACCESS.2025.3606572

Dželihodžić, A., Žunić, A., & Žunić Dželihodžić, E. (2024, June). Predictive modeling of stock prices using machine learning: A comparative analysis of LSTM, GRU, CNN, and RNN models. In International Symposium on Innovative and Interdisciplinary Applications of Advanced Technologies (pp. 447-467). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-71694-2_33

Ekundayo, F., Atoyebi, I., Soyele, A., & Ogunwobi, E. (2024). Predictive analytics for cyber threat intelligence in fintech using big data and machine learning. International Journal of Research Publication Review, 5(11), 1-15. https://doi.org/10.55248/gengpi.5.1124.3352

Goel, A., Garg, P., & Kumar, M. (2024). Decentralized finance: A catalyst for smart global value chains in future financial ecosystems. In Smart global value chain (pp. 198-211). CRC Press. https://doi.org/10.1201/9781003461432-13

Hasan, K., Hossain, F., Amin, A., Sutradhar, Y., Jeny, I. J., & Mahmud, S. (2025). Enhancing proactive cyber defense: A theoretical framework for AI-driven predictive cyber threat intelligence. Journal of Technologies Information. https://doi.org/10.55267/rtic/16176

Hossain, K. S., Ahmed, F., Akter, M., & Hossain, M. B. (2025). Artificial intelligence in transactional data analysis: A data-centric analysis of customer behavior in the USA.

Jawdhari, H. A., & Abdullah, A. A. (2021). A novel blockchain architecture based on network functions virtualization (NFV) with auto smart contracts. Periodicals of Engineering and Natural Sciences, 9(4), 834-844. https://doi.org/10.21533/pen.v9.i4.988

Jawdhari, H. A., & Abdullah, A. A. (2021). The application of network functions virtualization on different networks, and its new applications in blockchain: A survey. Management, 18, 1007-1044. https://doi.org/10.14704/WEB/V18SI04/WEB18179

Jawdhari, H. A., & Abdullah, A. A. (2022, November). New security mechanism of health data based on blockchain-NFV. In International Conference on New Trends in Information and Communications Technology Applications (pp. 230-247). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-35442-7_12

Kareem, C. M. (2025). A systematic review of security innovations in decentralized finance (DeFi) using blockchain technology. Informatica, 49(33). https://doi.org/10.31449/inf.v49i33.7990

Knutsson, H., & Engholm Flärd, M. (2025). Smart but vulnerable: Features that draw attackers to smart contracts.

Liao, H., Leng, S., Yang, J., Xu, J., Zhang, J., & Tang, J. (2024, March). A robust and efficient risk assessment framework for multi-step attacks. In 2024 7th International Conference on Information and Computer Technologies (ICICT) (pp. 309-314). IEEE. https://doi.org/10.1109/ICICT62343.2024.00056

Nahi, H. A., Fadhil, N. H., Saeed, M. M., & Salman, R. A. (2025). A novel blockchain-based system for developing a virtual judge. Journal of Computer Science, 21(2), 380-387. https://doi.org/10.3844/jcssp.2025.380.387

Nahi, H. A., Hashim, S. M., & Kreem, D. J. (2023). Blockchain for baccalaureate examination sheets protection in Iraq. Indonesian Journal of Electrical Engineering and Computer Science, 29(2), 1183-1191. https://doi.org/10.11591/ijeecs.v29.i2.pp1183-1191

Nahi, H. A., Khalid Ali, A., Ali Alaraji, M., Jawad Mohi, Z., Thamer Mahmood, N., Majed Mousa, A., Mohammed Saeed, M., & Almansoori, R. (2025). Blockchain network for regulation decentralized e-government systems. Data and Metadata, 4, 201. https://doi.org/10.56294/dm2025201

Nahi, H., Majed Mousa, A., Akeel Hamed, E., Khalid Ali, A., Jawad, S., Mahdi Abdulkadium, A., & Salman, R. A. (2025). Quantum key distribution for enabling secure network function vitalization orchestration over a network. Data and Metadata, 4, 202. https://doi.org/10.56294/dm2025202

Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2024). Data-driven cyber threat intelligence: Leveraging behavioral analytics for proactive defense mechanisms.

Paramasivan, A. (2024). Harnessing AI for behavioral insights: Unlocking the potential of transactional data. IJLRP-International Journal of Leading Research Publication, 5(10).

Parisi, C., & Budorin, D. (2024). DeFi security. In Web3 applications security and new security landscape: Theories and practices (pp. 3-18). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-58002-4_1

Pishdar, M., Lei, Y., Harfoush, K., & Manzoor, J. (2025). Denial-of-service attacks on permissioned blockchains: A practical study. Journal of Cybersecurity and Privacy, 5(3), 39. https://doi.org/10.3390/jcp5030039

Prajapati, C. (2025). Decentralized finance (DeFi) and cryptocurrencies: The latest thinking of people towards the blockchain and FinTech industry (Doctoral dissertation, University of the Cumberlands).

Sahu, K., & Kumar, R. (2024). A secure decentralised finance framework. Computer Fraud & Security, 2024(3). https://doi.org/10.12968/S1361-3723(24)70010-4

Sakthidevi, I., & Fathima, G. (2025). Threat-aware circular security in smart healthcare. In Digital forensics in next-generation internet for medical things: Balancing security and sustainability (p. 55). https://doi.org/10.1201/9781003640325-4

Shaikh, Z. M., & Ramadass, S. (2024). Unveiling deep learning powers: LSTM, BiLSTM, GRU, BiGRU, RNN comparison. Indonesian Journal of Electrical Engineering and Computer Science, 35(1), 263-273. https://doi.org/10.11591/ijeecs.v35.i1.pp263-273

Yaw, H. A. (2025). Risk management in decentralised finance (DeFi).

Zhang, Z., Xiao, G., Song, S., Aygun, R. C., Stavrou, A., Zhang, L., & Osterweil, E. (2024). Revealing protocol architecture's design patterns in the volumetric DDoS defense design space. IEEE Communications Surveys & Tutorials, 27(1), 353-371. https://doi.org/10.1109/COMST.2024.3392253

Zou, Z., Liu, Z., Zhao, L., & Zhan, Q. (2025). Blocka2a: Towards secure and verifiable agent-to-agent interoperability. arXiv preprint arXiv:2508.01332.