ARTblock: Blockchain-Integrated AI for Real-Time Transaction Authenticity Verification in Fintech

Irin Sultana , Syed Mustavi Maheen , Md Nasim Fardous Zim , Vijay Harikrishnan , Naresh Kshetri *

Posted Date: 4 November 2025

doi: 10.20944/preprints202511.0237.v1

Keywords: artificial intelligence; blockchain; fintech; machine learning; real-time verification; transaction security

 doi:10.20944/preprints202511.0237.v1

Article

ARTblock: Blockchain-Integrated AI for Real-Time Transaction Authenticity Verification in Fintech

Irin Sultana [1], Syed Mustavi Maheen [2], Nasim Fardous Zim [3], Vijay Harikrishnan [4] and Naresh Kshetri [5,*]

[1] School of Business & Technology, Emporia State University, Emporia, KS, USA
[2] School of Business & Tech, Emporia State University, Emporia, KS, USA
[3] School of Business & Technology, Emporia State University, Emporia, KS, USA,
[4] Department of Cybersecurity, Rochester Institute of Technology, Rochester, NY, USA
[5] Department of Cybersecurity, Rochester Institute of Technology, Rochester, NY, USA
* Correspondence: naresh.kshetri@ieee.org

Abstract

ARTblock is an innovative blockchain-based artificial intelligence platform designed to revolutionize real-time transaction authenticity verification in the financial technology industry. This novel methodology combines artificial intelligence and machine learning for advanced fraud detection, complemented by the immutability and transparency of blockchain technology. ARTblock presents a novel approach to enhancing security, efficiency, and scalability in financial transactions by integrating these two transformative technologies. The technology employs AI algorithms to analyze transaction patterns and detect anomalies in real-time, while recording and verifying this data on a distributed ledger. This collaboration creates a robust system capable of detecting and preventing fraudulent activities with exceptional accuracy and speed. ARTblock's unique architecture enables seamless growth, making it suitable for handling the increasing number and complexity of modern financial transactions. ARTblock includes real-time transaction monitoring, proactive fraud prevention, and the improvement of international transactions. In the realm of international payments, ARTblock addresses substantial challenges such as high fees, lengthy processing times, and regulatory compliance issues. The solution utilizes blockchain's inherent features to significantly reduce transaction costs and processing times, while AI ensures compliance with diverse regulatory standards. This study rigorously examines the architecture, implementation layers, and application domains of ARTblock, a blockchain-integrated AI system developed for the real-time verification of financial transactions. The proposed methodology provides critical insights for improving secure, scalable, and regulatory-compliant fintech systems through a hybrid technological framework.

Keywords: artificial intelligence; blockchain; fintech; machine learning; real-time verification; transaction security

1. Introduction

Maintaining the integrity and safety of real-time transactions in the fast-changing field of financial technology (Fintech) is still a big problem. Because of new, advanced cyber threats and fraud plans, we need strong, safe, and trustworthy proof systems that can work in real time (Saleh, 2024) [1]. Traditional ways of verifying transactions, which often depend on centralized systems, have major flaws like single points of failure, data corruption, and delay problems (Soori, Dastres, & Arezoo, 2023) [2]. So, to get around these problems successfully, new ideas based on cutting edge technologies have become necessary.

Blockchain technology, which is known for being autonomous, safe, and open, has shown a lot of promise in real-time situations for solving these security and authenticity problems. The properties of blockchain, such as immutability, openness, and decentralization, make sure that transactional

 doi:10.20944/preprints202511.0237.v1

data can't be changed or stolen once it's been recorded. This makes financial operations more reliable and real (Saleh, 2024; Biswas & Muthukkumarasamy, 2016) [1,3]. The distributed ledger technology (DLT) that blockchain is based on protects strongly against fraud, cuts down on wasteful operations, and makes sure that transactions are validated instantly (Puthal et al., 2018) [4].

At the same time, combining Artificial Intelligence (AI) with blockchain has become a game-changing method that makes transaction proof much safer, more accurate, and faster. With features like anomaly detection, predictive analytics, and pattern recognition, AI systems make it easy to spot fraud and illegal entry attempts right away (Soori et al., 2023) [2]. When AI algorithms are connected to blockchain, they can safely manage autonomous transaction data to quickly check its trustworthiness. This makes transactions more accurate and cuts down on the delay that comes with standard verification processes by a large amount (Lakhan et al., 2023; Mahmood & Jusas, 2021) [6].

New studies show that mixing blockchain and AI technologies can be very helpful. For example, Saleh (2024) highlights how decentralized AI, powered by blockchain, significantly improves cybersecurity measures through secure, transparent, and immutable data storage. Similarly, Soori et al. (2023) describes how AI-powered blockchain technology creates an autonomous platform for proactive maintenance and safe data management, which is very important for checking the accuracy of Fintech transactions in real time.

But it's not always easy to use AI and blockchain together in real-time financial apps. Problems with growth, sharing, and following the rules are big problems (Saleh, 2024; Almutairi et al., 2023) [7]. As a result, continuing research and development is necessary to solve these problems and make sure that combined blockchain and AI systems for real-time transaction verification work well.

This article presents "ARTblock," a blockchain-based AI system made specifically for checking the authenticity of transactions in real time in financial settings. ARTblock wants to improve transaction security, lower verification delay, and offer a strong, dependable, and decentralized way to fight complex financial frauds and cyber threats by using the ways that AI and blockchain work together.

2. Literature Review

The financial technology (Fintech) industry has been greatly affected by blockchain technology, which provides safe, open, and independent financial systems. This system uses a decentralized log to keep safe records of activities across a network of computers. This makes things safer and clearer (Nakamoto, 2009) [8]. In recent years, the blockchain has been used for more than just cryptocurrency in Fintech. It is now used for digital payments, supply chain finance, and asset management, among other things (Idrees et al., 2021) [9].

A number of studies have shown that blockchain can make financial deals safer and more reliable. For example, Biswas and Muthukkumarasamy (2016) talk about blockchain's role in using cryptography to make transactions safe and impossible to change. In the same way, the fact that blockchain data can't be changed has been studied a lot as a key benefit for protecting financial data from illegal changes and making sure that transactions are real (Emmadi & Narumanchi, 2017) [10]. Blockchain technology, especially when used in banking, has led to amazing new ideas. But along with this progress, there are rising worries about longevity, energy use, and environmental effects. Bitcoin mining is one example of this [11].

As it can manage huge amounts of data quickly and correctly, artificial intelligence (AI) is becoming more and more important to Fintech transaction verification systems. Real-time fraud discovery and prevention has gotten a lot better thanks to AI-driven methods like machine learning (ML) tools, anomaly detection, and prediction analytics (Zhang et al., 2021) [12].

By looking at patterns, trends, and behaviors, AI-based systems are very good at finding problems in banking activities. Recent research has focused on AI's ability to automate fraud detection processes, which would greatly reduce the amount of work that needs to be done by hand, speed up, and improve the accuracy of transactions (Rawat et al., 2022) [13]. Federated learning, a

 doi:10.20944/preprints202511.0237.v1

type of autonomous AI, lets several groups work together to train models without sharing private information. This keeps privacy and security safe [1].

The combination of blockchain and AI is a big step forward in making Fintech trade systems safer and more efficient. Blockchain is a safe, open, and unchangeable way to store data, and AI systems make it possible to quickly analyze data, find frauds in real time, and verify transactions automatically (Saleh, 2024) [1].

Recent studies have looked at different ways that blockchain and AI can work together, showing that they can help verify transactions in big ways. Lakhan et al. (2023) suggested using blockchain to power an AI framework that will improve safety in medical apps. This framework should focus on better data integrity and safe real-time processing. Similarly, Mahmood and Jusas (2021) show how blockchain-enabled shared learning can help with privacy issues in collaborative AI settings. This will show how blockchain and AI can be used together to make data more secure and private.

Even though there are a lot of promises, combining blockchain and AI technologies comes with a number of problems. Scalability is still a big issue because blockchain networks can have problems with delay and speed, which makes it hard to verify transactions in real time (Yang et al., 2020) [15]. Interoperability between different blockchain platforms and AI tools adds to the difficulties, making it harder for systems to share data and models without any problems (Belchior et al., 2021) [16].

Another important problem is following the rules set by regulators, especially when it comes to data safety and security. Existing legal systems might not be able to properly deal with the new technological ideas that blockchain and AI bring to the table. This means that regulations need to be constantly changed to keep up with new Fintech innovations (Yeoh, 2017) [17].

3. Real-Time Transaction Monitoring

Real-time transaction monitoring (RTTM) is an essential element in modern financial technology systems, especially when combined with blockchain and artificial intelligence. RTTM allows financial institutions to analyse transactions in real-time, offering immediate insights and enhancing security throughout the financial ecosystem (Hassan et al., 2022) [19].

3.1. Core Components of ARTblock's RTTM System

Modern blockchain-integrated RTTM systems consist of multiple essential components that collaborate to guarantee the authenticity and security of transactions. The data collection layer is responsible for capturing transaction data from various sources within the financial network. The AI processing engine analyzes transaction patterns through the application of advanced machine learning algorithms. The blockchain validation layer systematically documents authenticated transactions within a decentralized ledger. An alert management system is designed to generate notifications for activities that are deemed suspicious. Current blockchain-integrated RTTM systems consist of multiple essential components that collaborate to guarantee the authenticity and security of transactions. The data collection layer is responsible for capturing transaction data from various sources within the financial network. The AI processing engine analyzes transaction patterns through the application of advanced machine learning algorithms. The blockchain validation layer systematically documents authenticated transactions within a decentralized ledger framework. An alert management system is designed to generate notifications in response to suspicious activities.

 doi:10.20944/preprints202511.0237.v1

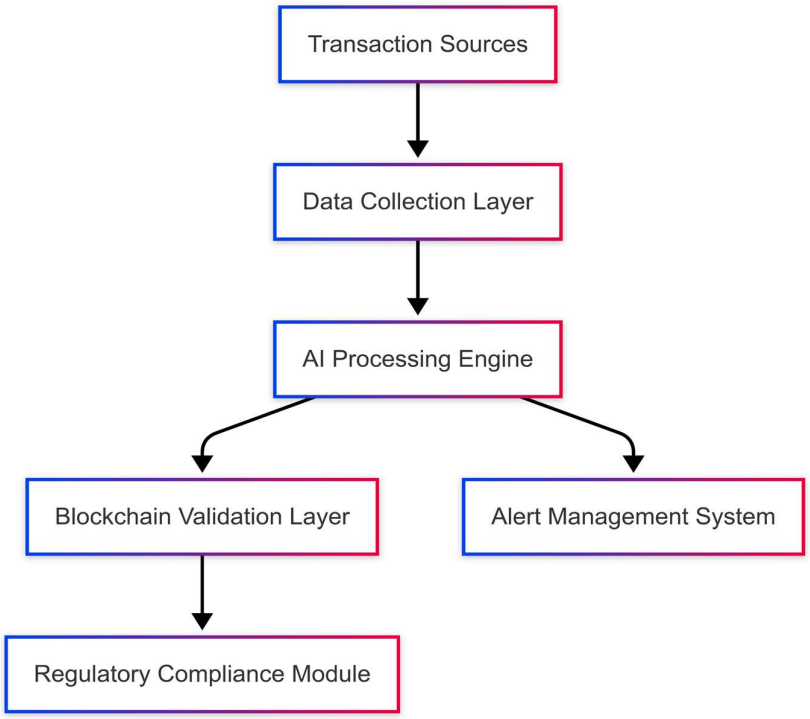

Figure 1. - Blockchain-Integrated RTTM System Architecture.

3.2. Advanced Data Processing Mechanisms

In blockchain-integrated RTTM systems, transaction data is subjected to various levels of analysis. According to the research conducted by (Ashfaq et al., 2022) [20], the integration of blockchain technology with artificial intelligence for transaction monitoring results in improved security within financial networks. The approach utilizes XGboost and Random Forest algorithms for transaction classification, with subsequent security measures applied through a blockchain network.

The data processing workflow in ARTblock follows the algorithm below:

Algorithm 1: Blockchain-AI RTTM Data Processing

Input: Transaction data stream T
Output: Verified transaction records V, Alerts A

1. Initialize empty sets V, A
2. For each transaction t in T:
    3. Extract features F from t
    4. Apply AI model M to F → confidence score c
    5. If c < threshold τ:
        6. Add t to A
        7. Initiate enhanced verification protocol
    8. Else:
        9. Record t on blockchain
        10. Add t to V
11. Return V, A

According to (Hassan et al., 2022) [19], blockchain-based RTTM systems need to balance accuracy with processing speed. This balance can be achieved by utilizing a distributed computing

 doi:10.20944/preprints202511.0237.v1

approach that parallelizes transaction verification across multiple nodes, reducing latency while maintaining high accuracy levels.

3.3. Integration with Existing Financial Systems

A significant challenge in implementing advanced RTTM systems is integration with legacy financial infrastructure. (Taher et al., 2024) and (Rane et al., 2023) highlight that successful blockchain-based fintech solutions require middleware layers that enable seamless connectivity with existing banking systems, payment gateways, and financial networks. This integration capability has been identified as a critical success factor for blockchain-based fintech solutions.

Table 1. compares traditional monitoring approaches with blockchain-integrated RTTM systems based on research by (Rane et al., 2023) [22].

Feature	Traditional RTTM	Blockchain-Integrated RTTM
Processing Speed	Batch-based	Real-time continuous
Data Immutability	Limited	Blockchain-secured
Adaptability	Rule-based	AI-driven adaptive
Scalability	Limited by the central server	Distributed architecture
Integration Capacity	Proprietary APIs	Open standards
Cost Efficiency	High maintenance	Reduced operational costs

4. Fraud Detection and Prevention

Financial fraud remains a significant challenge for financial institutions, as global losses attributed to fraud continue to rise annually. (biocatch, 2024)reports that approximately 73% of financial organisations are utilising AI for fraud detection, with a majority anticipating an increase in both financial crime and fraud activity in the forthcoming years. The combination of artificial intelligence and blockchain technology facilitates innovative methodologies for detecting and preventing fraud within the financial technology sector.

4.1. Multi-layered Fraud Detection Framework

Modern fraud detection systems that utilize blockchain technology implement a multi-layered strategy, integrating various complementary techniques. Pattern recognition employs machine learning models to detect anomalous transaction patterns by analysing historical data. Anomaly detection utilizes statistical analysis to identify transactions that diverge from predefined standards. Behavioural biometrics examines user behavior patterns for the purpose of identifying account takeovers. Network analysis investigates transaction networks to detect coordinated fraud attempts.

Recent research by (Ashfaq et al., 2022) demonstrates that multi-layered fraud detection approaches can significantly improve detection rates compared to single-method approaches. In their study, they integrated both XGBoost and Random Forest algorithms with blockchain technology to detect fraudulent transactions in cryptocurrency networks.

 doi:10.20944/preprints202511.0237.v1

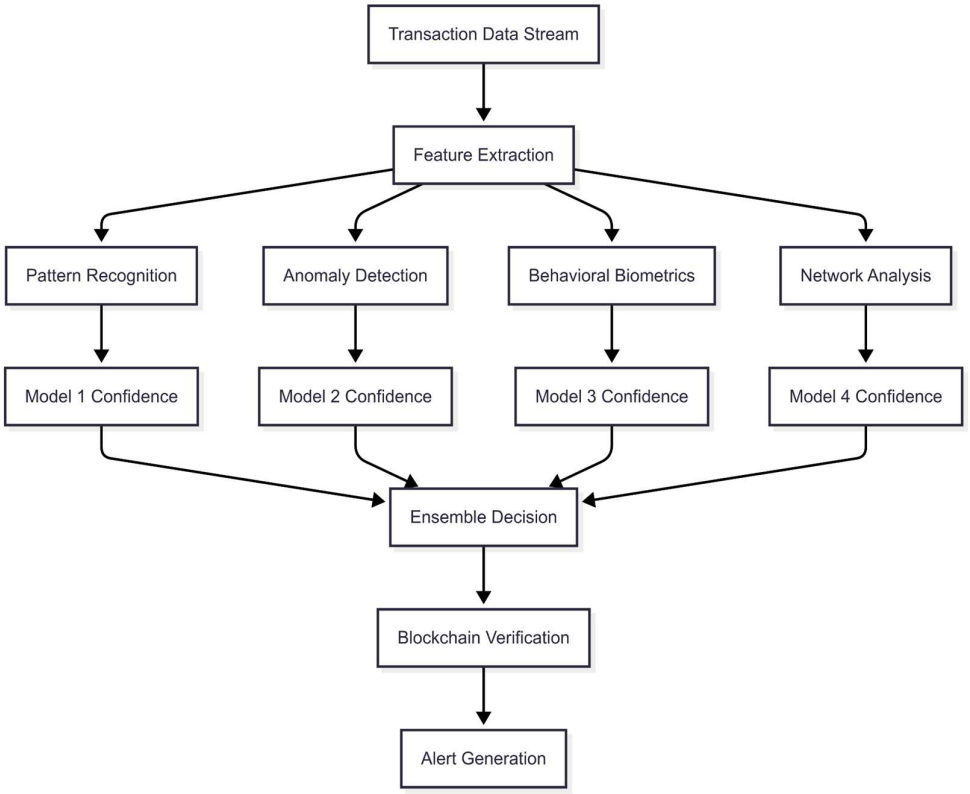

Figure 2. Multi-layered Fraud Detection Framework.

4.2. Machine Learning Models for Fraud Detection

The identification of fraudulent activity in current systems takes advantage of a wide range of machine learning techniques. With the use of labelled historical fraud data, supervised learning classification models are developed. In the absence of any prior labelling, unsupervised learning clustering algorithms can recognize irregular transaction patterns. With the use of deep learning neural networks, sophisticated fraud patterns may be captured across enormous datasets. When feedback is taken into consideration, adaptive reinforcement learning models increase detection skills.

(Ali, 2022) conducted a comprehensive evaluation that analyzed the efficacy of several machine learning algorithms for the detection of financial fraud. They found that ensemble methods, which include many models, produced the greatest accuracy and the lowest false positive rates when compared to individual models.

The following is a presentation of the pseudo-code for a typical blockchain-integrated fraud detection algorithm, which is based on findings from recent research:

Algorithm 2: Blockchain-AI Fraud Detection
Input: Transaction T, Historical Data H
Output: Fraud Probability Score F, Confidence Level C

1. Extract feature vector V from transaction T
2. For each model M in model ensemble:
   3. Compute preliminary score S_M = M(V, H)
4. Calculate ensemble score S_E = WeightedAverage(S_M for all M)
5. Apply calibration function to get F = Calibrate(S_E)
6. Compute confidence level C based on model agreement
7. If F > threshold_high:

 doi:10.20944/preprints202511.0237.v1

8. Block transaction and trigger immediate review
9. Else if F > threshold_medium:
10. Flag for post-transaction review
11. Record suspicion level on blockchain
12. Else:
13. Approve transaction
14. Record on blockchain with normal status
15. Return F, C

4.3. Blockchain's Role in Fraud Prevention

Based on the findings of (Rane et al., 2023) [22], the use of blockchain technology offers a number of significant benefits that are essential for the prevention of fraud. The use of immutable transaction records ensures that once transaction data has been captured, it cannot be changed, hence avoiding fraud that occurs after the fact. In order to validate transactions, distributed verification necessitates the use of numerous nodes, which in turn reduces the likelihood of hacked systems. The capabilities of a transparent audit trail ensure that every transaction is permanently documented and can be traced back to its origin. Contract execution may be automated by smart contract enforcement, which reduces the risks associated with intermediaries.

According to the findings of (Taher et al., 2024) and (Rane et al., 2023) [22], blockchain-based fraud protection systems that make use of ensemble learning approaches are capable of achieving fraud detection accuracy rates that are greater than 90%. This is especially true for unauthorized alterations and tampering with transactions.

4.4. Proactive Fraud Prevention Strategies

Modern blockchain-integrated systems use a number of proactive fraud protection methods in addition to monitoring for fraudulent activity. Authentication based on risk implements additional safety precautions for transactions that are considered to be high-risk. The process of continuous learning allows for the adaptation of new fraud patterns through continual model training. Through the use of cross-institutional data sharing, fraud indications may be safely shared among several financial institutions while maintaining confidentiality. To guarantee that all transactions are in accordance with regulatory regulations, regulatory compliance automation is utilized.

According to (biocatch, 2024) [23], despite the fact that 73% of organisations are utilizing AI for the purpose of fraud detection, 41% of anti-fraud decision-makers indicate that fraud and financial crime are handled in separate units with no cross-collaboration. This indicates that there is a significant amount of room for improvement in proactive fraud prevention approaches.

In conclusion, the combination of artificial intelligence with blockchain technology results in the creation of an all-encompassing method for the detection and prevention of fraudulent actions. This method is able to identify and prevent fraudulent activities with a high degree of accuracy and a small amount of false positives. The multi-layered design guarantees that it is resistant against a wide variety of fraud schemes, and its agility enables it to grow as new fraud patterns arise.

5. Cross-Border Transactions

Cross-border transactions imply financial exchanges or commercial operations conducted between entities situated in distinct nations. These transactions have grown progressively more common in the global economy, particularly due to the expansion of cross-border e-commerce. Liang et al. (2021) assert that cross-border e-commerce has emerged as a novel growth catalyst for worldwide foreign trade, especially in the post-pandemic period. In contrast to conventional trade, which predominantly depends on maritime transport, cross-border e-commerce transactions necessitate great efficiency in both maritime and terrestrial transport systems. The magnitude and efficacy of cross-border transactions are profoundly affected by the degree of trade facilitation among

 doi:10.20944/preprints202511.0237.v1

the involved nations. Trade facilitation includes methods that streamline and standardize international trade processes, consequently decreasing trade expenses and improving the overall trade climate. This encompasses enhancements in logistics infrastructure, customs clearance procedures, governmental governance systems, and cross-border logistics services.

Cross-border transactions encounter numerous obstacles, such as elevated fees, protracted processing durations, security vulnerabilities, and insufficient transparency. For example, consumer cross-border payments typically incur bank costs averaging more than 11%, but B2B payments encounter fees averaging 1.5% and processing delays of up to several weeks. The inefficiencies have resulted in considerable losses, as U.S. eCommerce companies faced an 11% failure rate in cross-border transactions in 2023, culminating in $3.8 billion in lost revenues (PYMNTS, 2024) [26]. Furthermore, cross-border transactions are essential to the global economy, with remittances to low- and middle-income nations exceeding $500 billion in 2020 (Liang et al., 2024) [25].

According to Rapid Innovation (2024) [27], Blockchain technology has emerged as a possible answer to these difficulties, with the potential to transform cross-border payments by lowering costs, improving security, and increasing efficiency. Blockchain-based systems can substantially reduce transaction costs, with estimations indicating a decrease of up to 80% relative to conventional techniques (PYMNTS, 2024) [26]. Moreover, blockchain facilitates near-instantaneous processing of cross-border payments continuously, devoid of intermediaries, potentially diminishing processing durations from days to seconds (ScienceSoft, 2018) [28].

The system improves security via multi factor authentication, end-to-end encryption, and tokenization while adhering to regulations such as PSD2, KYC, and AML requirements (KMS system, 2024) [29]. Real-time transaction monitoring systems, frequently connected with blockchain technologies, enhance security by analyzing transactions as they occur and promptly detecting suspect activities (Focal AI, 2025) [30]. The increasing adoption of blockchain for cross-border payments, driven by financial institutions, FinTechs, and central banks, is poised to revolutionize international money transfers by providing a more efficient, secure, and transparent alternative to conventional systems. Moreover, initiatives such as China's "Belt and Road" have intensified the integration of nations along the route with China's maritime economy, fostering cross-border e-commerce as a novel catalyst for global trade expansion (Liang et al., 2021) [25]. This has resulted in the adoption of numerous trade facilitation strategies, including the enhancement of marine economic conditions and the decrease of cross-border shipping and land transport expenses.

As cross-border transactions progress, emphasis is increasingly placed on enhancing delivery timeliness, minimizing trade expenses, and assuring adherence to rules such as PSD2, KYC, and AML mandates. Real-time transaction monitoring systems, frequently connected with blockchain technologies, enhance security by analyzing transactions as they occur and promptly detecting suspect activities (Focal AI, 2025) [30]. Qing et al. (2021) underscore the necessity of data mining tools for processing and analyzing transaction risks, forecasting future problems, and recommending specific risk mitigation strategies. This strategy can mitigate the risks linked to cross-border e-commerce transactions, which is especially vital considering the present condition of China's foreign trade volume in this sector, the absence of a specialized legal framework, and the comparatively low barriers to industry entry.

6. Security Enhancements Using ARTblock

Leveraging AI for enhanced security, analytical capabilities, and scalability is the urgent demand of modern cybersecurity as diverse organizational environments and IT infrastructure are backed by blockchain technology [32]. AI-driven IT infrastructure have significant improvements in reliability, speed, and accuracy of risk management, with the capability of addressing emerging cyber threats. The use of AI-generated images has other challenges in the content verification, media, and digital art that are almost the same as human-made images [33]. The use of Gray Level Co-occurrence Matrix (GLCM) features and Local Binary Patterns (LBP) for texture analysis has been done with deep learning architectures (VGG16, ResNet50). A comprehensive dataset from Hugging Face has

 doi:10.20944/preprints202511.0237.v1

provided the balanced foundation for model training (75K human-created images and 75K AI-generated images).

Despite the increasing number of online crimes, privacy & security concerns, and online cyber-bullying, Generative artificial intelligence (GAI) is opening new paths that are protective & resilient in the prevention and detection of cyberbullying [34]. AI-driven tools can reduce various cybercrimes across social media platforms and can improve the future of automation, manufacturing, cyber industry, and healthcare etc. Integrating blockchain technology with artificial intelligence (AI) frameworks as an innovative approach to deepfake detection and mitigation [35]. The utilization of blockchain features - decentralization and immutability to enhance the reliability of detection and security via the proposed framework, Blockchain-augmented AI (BAAI) framework.

There are several benefits of blockchain integration in healthcare, primarily for the protection of electronic medical records (EMRs). Integrating blockchain technology with advanced cybersecurity measures to address data security and interoperability with several blockchain characteristics for sensitive healthcare data [36]. There is a significant increase in personal safety and cybersecurity online due to digital identity, secure browsing, and social media account's privacy [37]. There is an urgent need to create cyber awareness via the integration of blockchain-based secure web habits in the current scenario. Co-writing with AI tools (as a security authentication) with personalization of AI writing to preserve authentic voice for all writing assistance tools powered by LLMs [38]. Illumination of authenticity in human AI co-creation with a focus on more process and authentic shelves (both source authenticity and content authenticity) via findings. Recent research shows that attackers are increasingly using stealthy, adaptable malware, emphasizing the necessity for flexible, privacy-enhancing technologies [41]. Solutions such as ARTblock, lightweight fusion models for low-resource NLP, privacy-first emotion AI, and graph-based fraud detection all help to create more safe, explainable, and scalable financial transaction platforms [42,43,44].

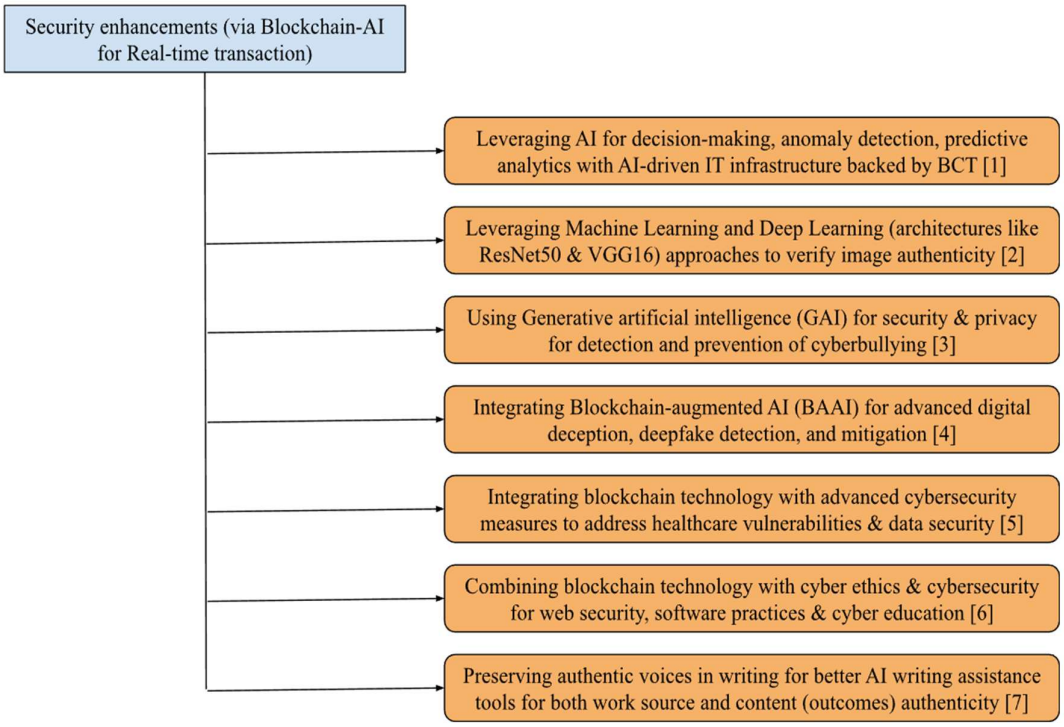

Figure 3. Security enhancements via Blockchain-integrated Artificial Intelligence (AI) for Real-time transaction authenticity verification – [37].

 doi:10.20944/preprints202511.0237.v1

7. Limitations, Conclusion and Future Scope

7.1. Limitations of the Study

Despite its innovative architecture and encouraging outcomes in simulations, the ARTblock platform has numerous technological and practical constraints. A significant challenge is scalability, particularly in high-frequency trading scenarios where delays in consensus or throughput limitations on blockchain networks might impair real-time performance. Moreover, interoperability continues to pose a significant barrier. Financial institutions utilize various legacy infrastructures and frequently adhere to proprietary data standards, rendering seamless integration with ARTblock significantly intricate and resource-demanding.

A further notable constraint arises from the regulatory framework. The AI algorithms in ARTblock rely on extensive data processing to accurately detect anomalies and fraudulent activities. Nonetheless, adherence to legislative frameworks such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and cross-border obligations like PSD2 and AML may limit data access or require expensive privacy-preserving measures. The dilemma between learning precision and data safety remains unaddressed. The system's environmental and computational burden, notably due to blockchain validation processes, raises issues over energy consumption and long-term sustainability, especially for public or hybrid blockchain implementations. Ultimately, ARTblock has not yet achieved comprehensive deployment across operational financial systems. The real-world robustness, stability against hostile threats, and cross-institutional operability remain unverified by comprehensive pilot projects or widespread industry adoption.

7.2. Conclusion

This study has introduced and rigorously analyzed ARTblock, an integrated platform that utilizes the advantages of blockchain and artificial intelligence to tackle the ongoing issues of real-time transaction authenticity in the financial technology sector. ARTblock utilizes a multilayered architecture to enhance fraud detection, anomaly identification, and transaction traceability, thereby safeguarding the integrity of various financial processes, ranging from local retail banking to cross-border remittances. ARTblock integrates supervised and ensemble machine learning models with blockchain's distributed ledger, enabling real-time validation of financial data independent of centralized authorities, thus enhancing transparency, minimizing operational latency, and bolstering trust.

The efficacy and adaptability of ARTblock are limited by systemic challenges associated with developing technologies, such as performance bottlenecks, standardization deficiencies, and compliance intricacies. These limits do not diminish the platform’s contributions but rather contextualize the boundary at which innovation must advance. ARTblock serves as a proof-of-concept and a fundamental model for decentralized and intelligent financial technology infrastructure. It advocates for hybrid security methods that are both technologically sound and flexible to changing legal and economic contexts.

7.3. Future Scope

Future study should focus on finding better ways to deal with these problems by making blockchains more scalable, making interoperability standards better, and improving regulatory systems. Looking into new agreement methods, like Proof of Authentication (Maitra et al., 2020) [18], could make blockchain work much better for real-time apps. Also, creating standardized frameworks and standards would make it easier for blockchain networks and AI models to work together, which would lead to more widespread use and better results in Fintech apps. In conclusion, combining blockchain and AI has a lot of benefits for making transactions more secure and true, but we need to solve the problems that come with it before we can fully use its potential. To make these combined

 doi:10.20944/preprints202511.0237.v1

solutions better and safer, and to make financial systems more open, efficient, and safe, research and development must go on all the time.

The future direction of ARTblock should concentrate on overcoming existing restrictions while enhancing its application through advanced technology integration and empirical validation. Initially, research should focus on improving scalability by investigating lightweight and adaptable consensus techniques, such as Proof of Authentication or pruning-based Directed Acyclic Graph (DAG) structures, to reduce latency and energy consumption. A crucial focus pertains to the standardization of interoperability protocols. Creating modular APIs and open formats would facilitate ARTblock's seamless integration across various banking systems and blockchain networks, hence fostering widespread use within the sector. Moreover, The combination of AI, emotion recognition, blockchain, and enhanced fraud detection is quickly improving real-time finance security. Continued research should concentrate on improving models for efficiency, transparency, and regulatory alignment in order to ensure trusted, robust financial infrastructures.

On the implementation front, executing multi-institutional pilot studies utilizing actual transaction logs, customer feedback mechanisms, and adaptive fraud scenarios will be essential for enhancing model calibration and robustness. ARTblock could be enhanced to integrate with decentralized identity frameworks, smart contract-based credit scoring, and tokenized asset validation systems, considering the increasing significance of data sovereignty and self-authenticating finance in the Web3 age. Subsequent revisions of ARTblock should prioritize energy-efficient blockchain processes. Incorporating climate-conscious ledger systems and implementing carbon-offset criteria during consensus validation may align the platform with international sustainability objectives. These advancements will transform ARTblock into a scalable, intelligent, and compliant financial trust infrastructure pertinent to the next generation of fintech ecosystems.

References

1. A. M. S. Saleh, "Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review," *Blockchain: Research and Applications*, vol. 5, no. 3, p. 100193, Feb. 2024, doi: https://doi.org/10.1016/j.bcra.2024.100193.
2. M. Soori, R. Dastres, and B. Arezoo, "AI-Powered Blockchain Technology in Industry 4.0, A Review," *Journal of Economy and Technology*, vol. 1, Jan. 2024, doi: https://doi.org/10.1016/j.ject.2024.01.001.
3. K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, Dec. 2016, doi: https://doi.org/10.1109/hpcc-smartcity-dss.2016.0198.
4. D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6–14, Jul. 2018, doi: https://doi.org/10.1109/mce.2018.2816299.
5. A. Lakhan, Mazin Abed Mohammed, J. Nedoma, R. Martinek, P. Tiwari, and N. Kumar, "Blockchain-Enabled Cybersecurity Efficient IIOHT Cyber-Physical System for Medical Applications," *IEEE Transactions on Network Science and Engineering*, pp. 1–14, Jan. 2022, doi: https://doi.org/10.1109/tnse.2022.3213651.
6. Z. Mahmood and V. Jusas, "Blockchain-Enabled: Multi-Layered Security Federated Learning Platform for Preserving Data Privacy," *Electronics*, vol. 11, no. 10, p. 1624, May 2022, doi: https://doi.org/10.3390/electronics11101624.
7. K. Almutairi *et al.*, "Blockchain Technology Application Challenges in Renewable Energy Supply Chain Management," *Environmental Science and Pollution Research*, Jan. 2022, doi: https://doi.org/10.1007/s11356-021-18311-7.
8. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *SSRN Electronic Journal*, 2008, doi: https://doi.org/10.2139/ssrn.3440802.

 doi:10.20944/preprints202511.0237.v1

9. S. M. Idrees, M. Nowostawski, R. Jameel, and A. K. Mourya, "Security Aspects of Blockchain Technology Intended for Industrial Applications," *Electronics*, vol. 10, no. 8, p. 951, Apr. 2021, doi: https://doi.org/10.3390/electronics10080951.
10. N. Emmadi and H. Narumanchi, "Reinforcing Immutability of Permissioned Blockchains with Keyless Signatures' Infrastructure," *Proceedings of the 18th International Conference on Distributed Computing and Networking*, Jan. 2017, doi: https://doi.org/10.1145/3007748.3018280.
11. M. I. Hossain, M. I. Hussain, A. Arobee, M. Nasim, and S. Akter, "Balancing Innovation and Sustainability: Learn the Potential Impact on the Environment of Bitcoin Mining," vol. 25, no. 1, Jan. 2025, doi: https://doi.org/10.62477/jkmp.v25i1.487.
12. Z. Zhang *et al.*, "Artificial intelligence in cyber security: research advances, challenges, and opportunities," *Artificial Intelligence Review*, vol. 55, no. 2, Mar. 2021, doi: https://doi.org/10.1007/s10462-021-09976-0.
13. B. S. Rawat, D. Gangodkar, V. Talukdar, K. Saxena, C. Kaur, and S. P. Singh, "The Empirical Analysis of Artificial Intelligence Approaches for Enhancing the Cyber Security for Better Quality," *IEEE Xplore*, Dec. 01, 2022. https://ieeexplore.ieee.org/abstract/document/10072877 (accessed Apr. 30, 2023).
14. A. Lakhan *et al.*, "Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare," *IEEE Journal of Biomedical and Health Informatics*, pp. 1–1, 2022, doi: https://doi.org/10.1109/jbhi.2022.3165945.
15. D. Yang, C. Long, H. Xu, and S. Peng, "A Review on Scalability of Blockchain," *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology*, Mar. 2020, doi: https://doi.org/10.1145/3390566.3391665.
16. R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A Survey on Blockchain Interoperability: Past, Present, and Future Trends," *ACM Computing Surveys*, vol. 54, no. 8, pp. 1–41, Nov. 2022, doi: https://doi.org/10.1145/3471140.
17. P. Yeoh, "Regulatory issues in blockchain technology," *Journal of Financial Regulation and Compliance*, vol. 25, no. 2, pp. 196–208, May 2017, doi: https://doi.org/10.1108/jfrc-08-2016-0068.
18. S. Maitra, V. P. Yanambaka, D. Puthal, A. Abdelgawad, and K. Yelamarthi, "Integration of Internet of Things and blockchain toward portability and low-energy consumption," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 6, Aug. 2020, doi: https://doi.org/10.1002/ett.4103.
19. Hassan, Muneeb Ul, et al. "Anomaly Detection in Blockchain Networks: A Comprehensive Survey." IEEE Communications Surveys & Tutorials, 2022, pp. 1–1, https://doi.org/10.1109/comst.2022.3205643.
20. Ashfaq, Tehreem, et al. "A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism." Sensors, vol. 22, no. 19, 21 Sept. 2022, p. 7162, www.mdpi.com/1424-8220/22/19/7162, https://doi.org/10.3390/s22197162.
21. Taher, Shimal Sh, et al. "Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach." Engineering, Technology & Applied Science Research, vol. 14, no. 1, 1 Feb. 2024, pp. 12822–12830, etasr.com/index.php/ETASR/article/view/6641/3442, https://doi.org/10.48084/etasr.6641.
22. Rane, Nitin, et al. "Blockchain and Artificial Intelligence (AI) Integration for Revolutionizing Security and Transparency in Finance." Social Science Research Network, 1 Dec. 2023, papers.ssrn.com/sol3/papers.cfm?abstract_id=4644253, https://doi.org/10.2139/ssrn.4644253.
23. Biocatch. "2024 AI Fraud Financial Crime Survey." Biocatch.com, 2024, www.biocatch.com/ai-fraud-financial-crime-survey.
24. Ali, Abdulalem. "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review." Applied Sciences, vol. 12, no. 19, 2022. MDPI, www.mdpi.com/2076-3417/12/19/9637/htm, https://doi.org/10.3390/app12199637.
25. Y. Liang, L. Guo, J. Li, S. Zhang, and X. Fei, "The Impact of Trade Facilitation on Cross-Border E-Commerce Transactions: Analysis Based on the Marine and Land Cross-Border Logistical Practices between China and Countries along the 'Belt and Road,'" *Water*, vol. 13, no. 24, p. 3567, Dec. 2021, doi: https://doi.org/10.3390/w13243567

 doi:10.20944/preprints202511.0237.v1

26. PYMNTS, "Cross-Border Payments Cost Could Be Cut by Blockchain, If It Can Only Solve the Scale Problem | PYMNTS.com," *PYMNTS.com*, Sep. 11, 2024. https://www.pymnts.com/blockchain/2024/cross-border-payments-cost-could-be-cut-by-blockchain-if-it-can-only-solve-the-scale-problem/
27. Rapid Innovation, "AI, Blockchain Solutions & Web3 Development Company," *Rapidinnovation.io*, 2024. https://www.rapidinnovation.io/post/revolutionizing-cross-border-payments-blockchain-2024
28. "Cross-Border Payments on Blockchain in 2023," *www.scnsoft.com*. https://www.scnsoft.com/blockchain/cross-border-payments
29. A. Minh, "Real-Time Payments: The Need for Speed in Fintech | KMS Technology," *KMS Technology*, Oct. 14, 2024. https://kms-technology.com/software-development/innovation/real-time-payments-the-need-for-speed-in-fintech.html (accessed Mar. 19, 2025).
30. "What is Real-Time Transaction Monitoring: Steps & Prevention," *Getfocal.ai*, 2025. https://www.getfocal.ai/blog/real-time-transaction-monitoring
31. H. Qing, G. Zheng, and D. Fu, "Risk Data Analysis of Cross Border E-commerce Transactions Based on Data Mining," *Journal of Physics: Conference Series*, vol. 1744, no. 3, p. 032014, Feb. 2021, doi: https://doi.org/10.1088/1742-6596/1744/3/032014.
32. Rahman, M. M., Pokharel, B. P., Sayeed, S. A., Bhowmik, S. K., Kshetri, N., & Eashrak, N. (2024). riskAIchain: AI-Driven IT Infrastructure—Blockchain-Backed Approach for Enhanced Risk Management. *Risks*, *12*(12), 206.
33. Ganokratanaa, T., Damnnoen, M., Katesomboon, P., Aiamphan, P., Maneeta, K., & Wattanapornprom, W. (2024, November). Human vs. AI: Leveraging Machine Learning and Deep Learning to Verify Image Authenticity. In *2024 28th International Computer Science and Engineering Conference (ICSEC)* (pp. 1-6). IEEE.
34. Rahman, M. M., Hossain, S., Bhusal, B., & Kshetri, N. (2025). Cyber AI Trends: Future Trends in AI for Cyberbullying Prevention. In *Combating Cyberbullying With Generative AI* (pp. 279-298). IGI Global Scientific Publishing.
35. Priya, M., Murugesan, J., Bhuvaneswari, P., Rubigha, M., Lalithambikai, S., & Mohanraj, B. (2024, September). Preserving Visual Authenticity: Block chain-Augmented AI Frameworks for Advanced Digital Deception Recognition and Mitigation. In *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 707-713). IEEE.
36. Pokharel, B. P., Kshetri, N., Sharma, S. R., & Paudel, S. (2025). blockHealthSecure: Integrating Blockchain and Cybersecurity in Post-Pandemic Healthcare Systems. *Information*, *16*(2), 133.
37. Chapagain, D., Kshetri, N., & Sihag, V. K. (2025). webCyberBlock: Cybersecurity and Cyber Ethics via Blockchain Technology–Need for Web Security, Software Practices, and End-User Cyber Education. In *Blockchain Technology for Cyber Defense, Cybersecurity, and Countermeasures* (pp. 123-138). CRC Press.
38. Hwang, A. H. C., Liao, Q. V., Blodgett, S. L., Olteanu, A., & Trischler, A. (2025). 'It was 80% me, 20% AI': Seeking Authenticity in Co-Writing with Large Language Models. *Proceedings of the ACM on Human-Computer Interaction*, *9*(2), 1
39. I. Sultana, Syed Mustavi Maheen, Asura Akter Sunna, and Naresh Kshetri, "SmSeLib: Smart & Secure Libraries - Navigating the Intersection of Machine Learning and Artificial Intelligence," pp. 118–123, Mar. 2025, doi: https://doi.org/10.1109/icict64582.2025.00025.
40. Naresh Kshetri, Mir Mehedi Rahman, Sayed Abu Sayeed, and I. Sultana, "cryptoRAN: A Review on Cryptojacking and Ransomware Attacks W.R.T. Banking Industry - Threats, Challenges, & Problems," May 2024, doi: https://doi.org/10.1109/incacct61598.2024.10550970.
41. N. Kshetri, I. Sultana, M. M. Rahman, and D. Shah, "DefTesPY: Cyber Defense Model with Enhanced Data Modeling and Analysis for Tesla Company via Python Language," *Ieee.org*, 2015, doi: https://doi.org/10.1109/ETNCC63262.2024.10767532.
42. Syed Mustavi Maheen, M. R. Faisal, and R. Rahman, "Alternative non-BERT model choices for the textual classification in low-resource languages and environments," pp. 192–202, Jan. 2022, doi: https://doi.org/10.18653/v1/2022.deeplo-1.20.
43. Syed Mustavi Maheen, I. Sultana, Naresh Kshetri, and M. Nasim, "emoAIsec: Fortifying Real-Time Customer Experience Optimization with Emotion AI and Data Security," pp. 793–798, Mar. 2025, doi: https://doi.org/10.1109/icmlas64557.2025.10968798.

 doi:10.20944/preprints202511.0237.v1

44. I. Sultana, S. M. Maheen, N. Kshetri, and M. N. Fardous Zim, "detectGNN: Harnessing Graph Neural Networks for Enhanced Fraud Detection in Credit Card Transactions," *2025 13th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1–6, Apr. 2025, doi: https://doi.org/10.1109/isdfs65363.2025.11011957.