Cryptography Converges with AI in Financial Systems: Safeguarding Blockchain Transactions with AI

Md. Nizamuddin[1*], Krishna Devarapu[2], Abhishake Reddy Onteddu[3], RamMohan Reddy Kundavaram[4]

[1]Faculty of Business and Economics, Universiti Malaya, Kuala Lumpur, Malaysia
[2]Senior Data Solutions Architect, Mission Cloud Services Inc., Beverley Hills, CA, USA
[3]Cloud DevOps Engineer, Pearson, Chicago, IL, USA
[4]Senior full Stack Developer (MERN-Stack), Silicon Valley Bank, Arizona Tempe, Chicago, IL, USA

*E-mail for correspondence: nizamuddin.prc@gmail.com

https://doi.org/10.18034/abr.v12i3.742

ABSTRACT

This paper examines how encryption and AI protect financial blockchain transactions. As blockchain technology grows more important in decentralized finance, AI must be included to solve cybersecurity issues. The research focuses on how AI improves cryptography systems, blockchain-based financial operations, and transaction security. Secondary data from the literature, peer-reviewed publications, and case studies are analyzed to synthesize AI-blockchain cryptography expertise. AI provides real-time anomaly identification, fraud prevention, predictive analytics, consensus mechanism optimization, and key management improvements, boosting blockchain security. Traditional cryptography methods become more adaptable and robust to emerging threats using AI. According to the research, the computational complexity of AI-driven solutions and AI model biases are constraints. Regulatory frameworks must be modified to ensure transparency, accountability, and compliance with AI-enhanced cryptography systems. This research shows that AI can strengthen blockchain transactions, indicating that AI and cryptography will shape safe and efficient financial systems in the future.

Key words: Cryptography, Artificial Intelligence, Blockchain, Financial Systems, Blockchain Security, Fraud Detection, Cryptographic Algorithms, Decentralized Finance (DeFi)

INTRODUCTION

Blockchain and AI have transformed the financial landscape in recent years. Cryptography, the blockchain underpinning, has protected digital transactions by ensuring data integrity, secrecy, and authenticity (Ahmmed et al., 2021; Allam, 2020; Boinapalli, 2020; Deming et al., 2021; Devarapu, 2020; Talla et al., 2021). However, new issues require creative cryptographic solutions as economic systems become more digital and complex. The confluence of AI and cryptography is crucial to blockchain-based financial transaction security and efficiency (Devarapu, 2021; Talla et al., 2021).

Decentralized blockchain systems have transformed the banking industry by eliminating intermediaries, lowering transaction costs, and providing transparency (Gade et al., 2021; Gummadi et al., 2020; Narsina et al., 2019; Onteddu et al., 2022; Gummadi et al., 2021; Kamisetty et al., 2021; Karanam et al., 2018; Kommineni et al., 2020; Kothapalli, 2021; Talla et al., 2022; Devarapu et al., 2019). These systems are safe because cryptography uses encryption protocols, digital signatures, and hash functions to provide trustless settings. Despite its sturdy architecture, blockchain is vulnerable. Quantum computing, data breaches, and consensus mechanism abuse threaten blockchain transaction security (Kommineni, 2019; Sridharlakshmi, 2021). This requires a paradigm shift—integrating AI-driven methodologies with cryptographic principles to solve shifting security concerns and adapt to the threat environment.

AI excels in pattern recognition, anomaly identification, and predictive analytics. It can improve blockchain cryptographic procedures, identify and prevent fraud, manage keys, and scale transaction verification. AI algorithms may identify bad actors manipulating consensus mechanisms like proof-of-work mining pools or foresee zero-day flaws in cryptographic schemes (Kommineni, 2020; Kothapalli et al., 2019; Kundavaram et al., 2018; Manikyala, 2022; Narsina, 2020; Rodriguez et al., 2020; Sridharlakshmi, 2020). AI can also monitor complicated networks, detect abnormalities in real-time, and react to new threats without human involvement, improving blockchain security (Narsina et al., 2021; Rodriguez et al., 2019). The rise of blockchain in financial systems matches the confluence of encryption and AI. Blockchain applications in decentralized finance (DeFi), central bank digital currencies (CBDCs), and cross-border payments must be resilient against sophisticated cyberattacks (Talla et al., 2021). This connection reduces fraud risks, speeds up transactions, and builds user confidence for financial institutions. However, combining AI with encryption raises ethical and technological issues such as algorithmic biases, data privacy, and the need for explainable AI systems for openness and accountability.

This article examines how encryption, AI, and financial systems interact to protect blockchain transactions. This convergence creates technology synergies, financial system applications, and problems that must be handled to maximize its potential. This report examines case studies, trends, and implementations to show how AI-driven cryptography solutions may safeguard blockchain-based financial systems. AI-cryptography integration is essential for safe and scalable blockchain technology in financial institutions. Understanding and harnessing the synergy between these two disciplines will strengthen financial systems against future dangers and generate new possibilities as the economic environment becomes more digital and decentralized.

STATEMENT OF THE PROBLEM

The increasing deployment of blockchain technology in financial institutions has transformed transaction recording, security, and behavior. Blockchain's trustless, decentralized nature relies on encryption to secure data integrity, secrecy, and authenticity. Blockchain technology is resilient but struggles to solve sophisticated cyber threats, scalability concerns, and financial transaction complexity. Advanced attack vectors and quantum computing threaten blockchain transactions, making standard encryption approaches ineffective (Thompson et al., 2019; Venkata et al., 2022; Onteddu et al., 2020). Innovative solutions are needed to protect blockchain transactions.

Current blockchain security research focuses on improving cryptographic methods and consensus processes. Despite their effectiveness, these initiatives typically lack the agility to combat new cyber threats in real-time. Many cryptographic protocols are static, making them susceptible to zero-day flaws and dynamic attacks. The expanding use of blockchain in decentralized finance (DeFi), cross-border payments, and central bank digital currencies (CBDCs) has increased security issues. Despite blockchain's growing use in financial institutions, little study has examined AI's synergistic ability to solve these complex problems (Richardson et al., 2021). This is a key research need since AI has shown transformational skills in anomaly detection, pattern recognition, and predictive modeling that might strengthen blockchain security frameworks.

Integrating AI into cryptography procedures may solve these issues. AI can scan massive amounts of information, discover real-time abnormalities, and react to new threats to develop a more dynamic and resilient blockchain security architecture (Roberts et al., 2020). Despite this agreement, essential problems remain: How can cryptographic systems combine AI to secure blockchain? What AI applications protect blockchain-based financial transactions? What ethical and computational hurdles must be overcome to actualize this potential? These concerns have not been thoroughly studied, highlighting the need for a dedicated study on AI and cryptography in financial systems.

This paper examines how encryption and AI secure blockchain transactions in financial institutions. It seeks to identify and solve the drawbacks of standard cryptographic methods, discuss how AI may improve blockchain security, and provide frameworks or methodologies that incorporate AI-driven solutions into cryptography. The article examines this interaction to show how financial systems use both domains' capabilities to develop durable and scalable blockchain infrastructures. Financial institutions must implement safe and scalable blockchain solutions in a quickly changing threat environment, making the challenge strategic and technical. This paper fills the research vacuum by analyzing how AI may be used to solve fundamental blockchain weaknesses and create more safe, efficient and trustworthy financial ecosystems. This project intends to advance blockchain security understanding and provide practical answers for the financial sector's future demands.

METHODOLOGY OF THE STUDY

This secondary data-based research examines how encryption and AI protect blockchain transactions in financial institutions. Research involves a thorough literature examination of peer-reviewed journal articles, conference proceedings, technical reports, and white papers. The report synthesizes past research to demonstrate the limits of existing cryptography methods, the promise of AI in blockchain security, and the problems of integrating these technologies into financial institutions. Data is qualitatively evaluated to comprehend the theoretical and practical ramifications of AI-driven cryptography solutions. This review critically examines case studies, emerging trends, and experimental results to consolidate knowledge and identify research needs. This method gives a thorough overview of the issue and a solid foundation for assessing AI's potential to improve blockchain-based financial systems.

Foundations of Blockchain Cryptography and Security

Blockchain technology, which offers a decentralized, transparent, and impenetrable transaction foundation, has completely changed the financial environment. Cryptography, which guarantees blockchain networks' security, integrity, and reliability, is at the heart of this technology. Important blockchain properties like immutability, anonymity, and data security are based on cryptography. This chapter examines the basic ideas of blockchain cryptography and its applications and constraints in financial systems (Niranjanamurthy et al., 2019).

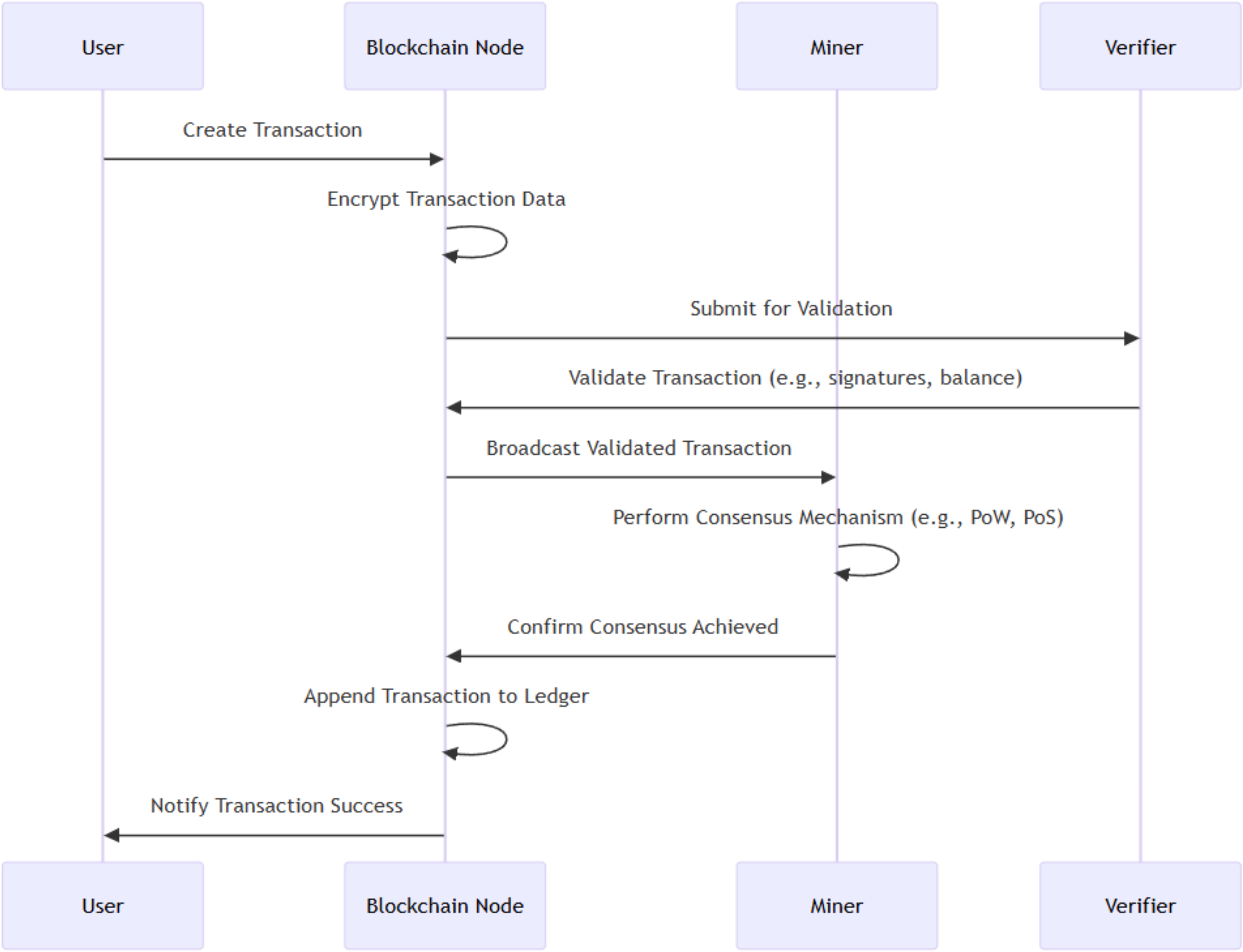
User
Blockchain Node
Miner
Verifier
Create Transaction
Encrypt Transaction Data
Submit for Validation
Validate Transaction (e.g., signatures, balance)
Broadcast Validated Transaction
Perform Consensus Mechanism (e.g., PoW, PoS)
Confirm Consensus Achieved
Append Transaction to Ledger
Notify Transaction Success
User
Blockchain Node
Miner
Verifier

Figure 1: Blockchain Transaction Security Workflow

The four leading players in securing a blockchain transaction are the user, Miner, blockchain node, and verifier, as shown in the sequence diagram in Figure 1. The user creates a transaction at the start of the process, and encryption comes next. To ensure everyone on the network agrees, the Blockchain Node verifies the transaction before the Miner participates in the consensus process. The transaction is added to the blockchain ledger when consensus is reached, guaranteeing its security and immutability.

Key Cryptographic Principles in Blockchain: Public-key cryptography and hashing are the two main methods of encryption used in blockchain systems. Hashing protects data integrity using cryptographic hash functions like SHA-256 to transform inputs into fixed-length outputs. Since each block in a blockchain includes the hash of the one before it, hashes are essential for connecting blocks in a chain. Any modification to a block changes its hash, upsetting the chain as a whole and indicating tampering. This architecture guarantees immutability. Asymmetric encryption, often known as public-key cryptography, uses key pairs—a private key for decryption and a public key for encryption—to enable safe transactions. Digital signatures, which verify transactions and authenticate users without disclosing private keys, are based on this technique. A user's private key is used to sign a transaction when they start it, and their public key is used to confirm the signature. Authenticity and non-repudiation are ensured by this cryptographic procedure, which is crucial for financial systems (Xiao-Ling et al., 2019).

Consensus Mechanisms and Security: Blockchain consensus procedures, which guarantee network members' agreement on the legitimacy of transactions, are also made possible by cryptography. Well-known techniques like Proof of Work (PoW) and Proof of Stake (PoS) depend on cryptographic methods to protect the network. For instance, PoW employs hash function-based computational puzzles that miners must solve to add blocks to the chain. In contrast, using cryptographic principles, PoS assigns validation privileges according to a participant's stake in the network. These safeguards make it difficult for bad actors to breach the system and stop double-spending.

Limitations of Cryptography in Blockchain Security: Blockchain cryptography has problems despite its advantages. The rise of quantum computing, which poses a danger to established cryptographic techniques like RSA and ECC (Elliptic Curve Cryptography), is one of the main issues. The mathematical issues underlying these algorithms might be effectively resolved by quantum computers, jeopardizing the security of blockchain technology. Cryptographic systems are also susceptible to human mistakes and technical errors. Blockchain systems may be vulnerable to assaults due to inadequate key management procedures or poorly thought-out algorithms. Furthermore, even if consensus processes are strong, they are vulnerable to assaults, such as 51% attacks, in which a malevolent actor takes over most of the network (Abdullah & Faizal, 2018).

Need for Enhanced Security Solutions: Strong security is essential as financial institutions increasingly use blockchain for cross-border payments and decentralized finance (DeFi) applications. Traditional cryptography techniques' static nature restricts their capacity to adjust to changing threats. This calls for cutting-edge techniques like artificial intelligence to improve blockchain security. The weaknesses in cryptographic systems may be mitigated by AI's real-time anomaly detection, predictive analysis, and adaptive learning capabilities (Zheng et al., 2019).

Cryptography, which provides data protection and transaction validation tools, is the foundation of blockchain security. However, its drawbacks highlight the need for sophisticated, AI-driven solutions to protect blockchain transactions in financial institutions, especially in light of new threats. This confluence of AI and cryptography might redefine blockchain security paradigms.

AI-Driven Enhancements in Blockchain Transactions

Combining blockchain technology with artificial intelligence (AI) offers a revolutionary chance to solve security issues and enhance blockchain-based financial systems. Blockchain's hitherto static security frameworks may be dynamically enhanced because of AI's sophisticated pattern recognition, anomaly detection, and predictive analytics skills. This chapter examines how blockchain transactions may be improved by AI-driven solutions that fortify security, boost operational effectiveness, and fix new vulnerabilities in financial systems.

The data from the Figure 2 Quadruple Bar Graph shows how AI is affecting the Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA), and Delegated Byzantine Fault Tolerance (dBFT) consensus processes used in blockchain technology. The Y-Axis shows progress metrics expressed as percentages of improvement in four dimensions: speed, energy consumption, accuracy, and security. The consensus mechanisms are listed on the X-axis, and the improvements in each measure are shown by four bars for each method. This graph compares how AI improves each measure for various consensus methods.

Real-Time Anomaly Detection and Fraud Prevention: AI's real-time anomaly detection capability is one of its most important contributions to blockchain security. AI-driven models can track transaction trends and spot oddities that point to fraud, such as attempts at double-spending or tampering with consensus processes. AI systems can notify network users of possible hazards and enable prompt actions by examining past data and identifying departures from typical behavior. For instance, machine learning algorithms trained on transaction datasets may detect suspicious actions like wash trading in decentralized finance (DeFi) systems or illegal efforts to get private keys. These algorithms provide a proactive line of protection by continually learning from fresh data and adjusting to the changing strategies of malevolent actors (Makridakis & Christodoulou, 2019).

Enhancing Consensus Mechanisms with AI: Although they are essential to blockchain security, consensus algorithms like Proof of Work (PoW) and Proof of Stake (PoS) have issues with scalability and efficiency. AI can improve these methods by anticipating the best routes for block validation and reducing computational costs. For example, conventional consensus protocols' energy consumption may decrease using reinforcement learning methods to determine which nodes are most effective for transaction validation. Additionally, AI may lessen consensus system weaknesses. AI algorithms can keep an eye on stake distributions and guarantee fair participation from all network nodes in PoS networks, which are susceptible to centralization. Similarly, AI can detect and flag mining pools in PoW systems that could be trying to dominate processing power, averting possible 51% assaults.

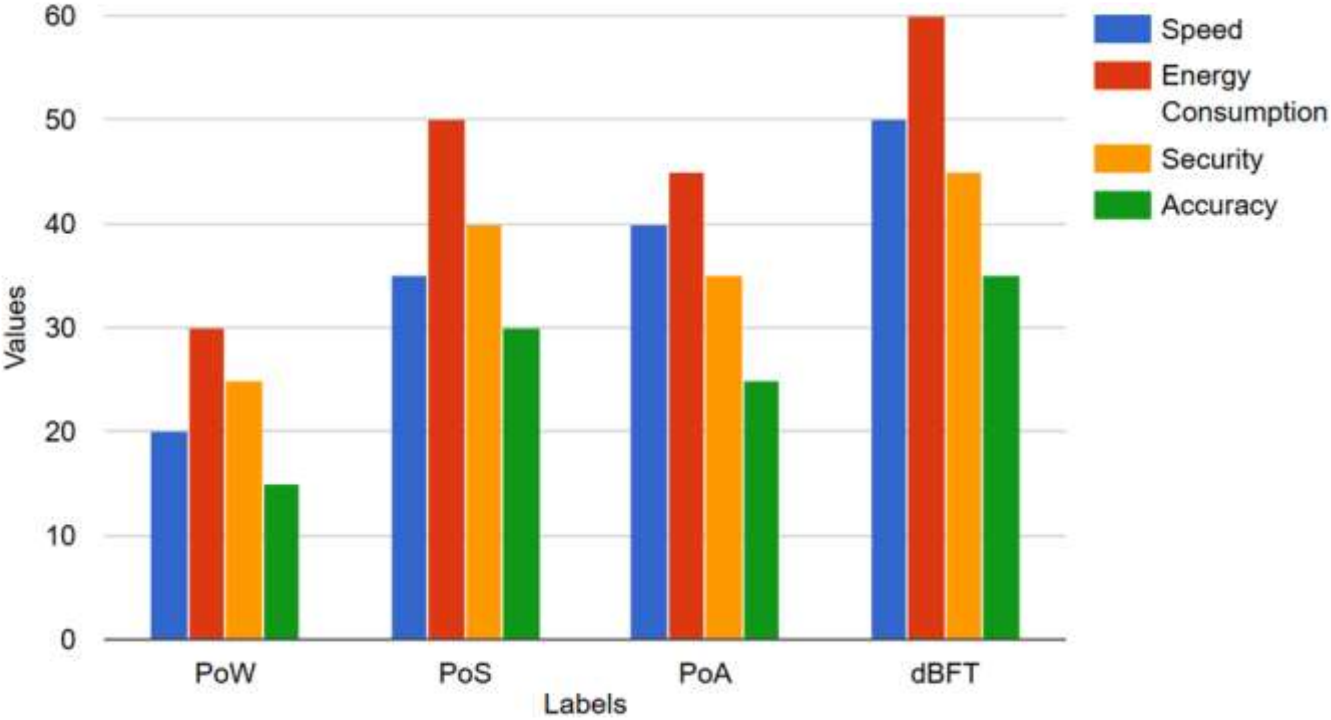

Figure 2: Impact of AI on Consensus Mechanisms

Key Management and Cryptographic Enhancements: Blockchain systems' private key management security may be significantly enhanced by AI. Conventional key storage techniques are vulnerable to malware and phishing assaults, as well as human mistakes. AI-driven solutions, including behavior-based access restrictions and biometrics, provide advanced techniques for safe key management. Artificial intelligence (AI) systems can identify and stop unwanted access by examining user behavior and improving cryptographic security. Furthermore, AI may advance post-quantum cryptography by aiding in creating and testing algorithms that are immune to the dangers posed by quantum computing. The creation of quantum-resistant cryptographic protocols may be accelerated by using machine learning models to assess how resilient suggested algorithms are to different types of attacks (Gurtu & Johny, 2019).

Predictive Analysis and Network Optimization: Blockchain systems can foresee possible network bottlenecks, improve transaction throughput, and lower latency thanks to AI's predictive analytics capabilities. AI, for instance, can predict transaction volumes at busy times, enabling the network to distribute resources and keep everything running smoothly. Furthermore, network optimization driven by AI guarantees the scalability and resilience of blockchain systems. Artificial intelligence (AI) improves blockchain systems' overall efficiency and dependability by dynamically modifying factors like block size and transaction fees depending on real-time data (Song et al., 2019).

AI-powered improvements provide a potent addition to cryptographic techniques for securing blockchain transactions. AI addresses the shortcomings of conventional blockchain security frameworks, making it possible to identify fraud in real-time, optimize consensus processes, and enhance cryptographic techniques. AI integration will be essential to building robust, scalable, and secure platforms to resist contemporary cyber threats' complexity as financial institutions embrace blockchain technology. In an increasingly digitized world, this combination of blockchain and artificial intelligence is a significant step toward maintaining the integrity of financial institutions.

Integrating Cryptography and AI in Finance

The growing use of blockchain technology in the financial industry has made strong security frameworks that can survive complex cyberattacks and guarantee operational effectiveness necessary. Blockchain systems traditionally rely on cryptography to protect transaction authenticity and data integrity. However, combining artificial intelligence (AI) with cryptography systems is becoming a ground-breaking method of strengthening financial systems as blockchain applications grow and cyber threats change. The practical use of AI and cryptography in finance is examined in this chapter, focusing on how they might work together to improve security, streamline procedures, and build confidence in blockchain transactions.

AI-Enhanced Cryptographic Security: AI has much to offer in overcoming the drawbacks of conventional cryptography techniques. Although data secrecy and integrity are guaranteed by cryptography, its static methods are often exposed to emerging and adaptive attacks. By offering dynamic, data-driven procedures to identify and address flaws, artificial intelligence (AI) improves cryptography systems. Large transaction databases, for example, may be analyzed by machine learning algorithms to find trends and highlight irregularities that may be signs of fraud or data breaches. AI may also be used to help make cryptography algorithms stronger. AI plays a key role in creating and verifying post-quantum cryptography protocols in the context of dangers posed by quantum computing. Adopting quantum-resistant systems, crucial for safeguarding blockchain-based financial applications, may be accelerated using AI-driven simulations to determine how resilient cryptographic techniques are against quantum assaults (Justinia, 2019).

Optimizing Blockchain-Based Financial Processes: Beyond security, process optimization in financial systems is another area where AI is integrated with cryptography systems. Scalability issues, transaction latency, and high consensus mechanism energy consumption are common problems for blockchain networks. These problems may be resolved by AI-driven optimization techniques that enhance transaction verification and resource allocation. Reinforcement learning methods, for instance, may improve node selection in blockchain consensus protocols, lowering computing costs and guaranteeing quicker transaction validation. Blockchain systems are more scalable and efficient because of AI's capacity to forecast network traffic and control resource allocation, which makes them more appropriate for large-scale financial transactions (Sgantzos & Grigg, 2019).

Strengthening Key Management and User Authentication: Secure private key management is one of the main issues with blockchain systems. Conventional techniques for keeping and retrieving private keys are susceptible to malware, phishing, and human mistakes. Artificial intelligence (AI) improves cryptographic key management by providing intelligent, behavior-based authentication methods. Using biometrics and user behavior analysis, these systems offer multi-factor authentication, lowering the possibility of unwanted access. Furthermore, by identifying odd patterns in user behavior, AI can stop illegal efforts to breach cryptographic systems. Cryptographic systems are protected from new threats by taking a proactive approach to security, and user authentication is strengthened.

Building Trust and Transparency in Financial Systems: Building trust and transparency is one of the most significant issues facing financial institutions, and the combination of AI and encryption addresses it. Financial institutions can show that they comply with regulations thanks to AI-driven monitoring tools that provide real-time insights into blockchain transactions. While AI offers the analytical skills to preserve transparency without sacrificing privacy, cryptographic techniques guarantee that transaction data stays safe and verifiable. Blockchain-based financial systems are made more trustworthy by the combined strength of AI and encryption, which automates fraud detection, risk assessment, and compliance monitoring. This trust becomes more important as financial institutions embrace innovations like tokenized assets, cross-border payment systems, and decentralized finance (DeFi) (Ravindran, 2019).

Table 1: Comparison of Traditional Cryptography vs. AI-Enhanced Cryptography

Aspect	Traditional Cryptography	AI-Enhanced Cryptography
Threat Adaptability	Static	Dynamic, real-time adaptation
Fraud Detection	Limited	Enhanced with anomaly detection
Computational Overhead	Moderate	Higher (AI algorithms)
Resilience to New Threats	Limited	Predictive and proactive

Table 1 lists the main distinctions between traditional cryptography methods and those augmented by artificial intelligence. It may concentrate on scalability, threat detection, computing demands, and flexibility.

Using AI and cryptography in the financial sector is a revolutionary step toward resolving the challenges of safeguarding blockchain transactions. Financial systems may attain improved security, efficiency, and transparency by fusing the advantages of cryptographic techniques with AI's flexibility and analytical powers. In an increasingly digital economy, this collaboration strengthens blockchain platforms against changing threats and opens the door for more reliable and robust financial ecosystems.

MAJOR FINDINGS

The paper provides critical insights into how encryption and AI protect blockchain transactions in financial institutions. The report synthesizes research and explores the synergies between these technologies to show how this integration tackles fundamental blockchain security concerns, streamlines financial operations, and builds more resilient financial ecosystems.

Enhanced Blockchain Security through AI Integration: AI improves blockchain security, which is a significant discovery. Traditional cryptography is resilient but cannot adapt to dynamic and sophisticated cyber threats like zero-day attacks and quantum computing. AI's real-time anomaly detection and massive dataset analysis provide adaptive protection against static cryptography techniques. Machine learning algorithms can detect double-spending and consensus process manipulation faster and more accurately than human techniques. AI helps create quantum-resistant cryptography algorithms. AI-driven simulations and testing frameworks speed the design and validation of quantum-resistant cryptography systems in the face of quantum computing. This proactive strategy maintains blockchain platform security over time in crucial applications like decentralized finance (DeFi) and central bank digital currencies.

Optimization of Blockchain Processes: AI's optimization of blockchain-based financial procedures is another noteworthy result. Blockchain systems struggle with scalability, energy consumption, and transaction verification delays. Advanced AI optimization methods include predictive analytics and reinforcement learning to improve resource allocation and transaction processing. AI algorithms can detect blockchain network bottlenecks, estimate transaction volumes, and dynamically distribute compute resources to ensure smooth operations during peak times. AI improves PoW and PoS efficiency by improving node selection and network health. AI makes blockchain networks more sustainable and suited for high-volume financial transactions by lowering computational overhead and energy use.

Strengthened Key Management and User Authentication: According to the research, AI enhances private key management and user authentication, which are crucial blockchain security measures. Traditional key storage techniques endanger financial systems from theft and human mistakes. AI improves security with biometric and user behavior authentication. To protect cryptographic keys and user credentials, these systems detect unwanted access attempts in real-time and react to new threats.

Trust and Transparency in Financial Ecosystems: AI-driven monitoring solutions give real-time blockchain transaction insights for financial system transparency and compliance. AI technologies identify unusual transaction patterns and enforce regulatory norms, while cryptography protects data. This integration shows stakeholders that blockchain-based financial systems are trustworthy and accountable.

The results show that encryption and AI can alter financial institutions. This confluence improves blockchain security, operational efficiency, trust, and transparency. As financial institutions adopt blockchain technology, encryption, and AI provide a solid framework for tackling emerging difficulties and creating safe, scalable, and trustworthy financial ecosystems.

LIMITATIONS AND POLICY IMPLICATIONS

Cryptography and AI improve blockchain transaction security, but there are limits. The computational complexity of AI-driven solutions is a significant issue. In high-volume financial systems, real-time anomaly detection and machine learning models might need a lot of processing power, causing scalability challenges and higher expenses. AI models pose accuracy and bias problems that compromise security.

To accommodate blockchain systems using AI and cryptography, regulatory frameworks must change. AI-driven encryption solutions may be too complicated for current standards, creating compliance and oversight holes. Policymakers must establish AI standards that assure openness, justice, and accountability while protecting cryptographic security and privacy. Regulators, financial institutions, and technology suppliers must work together to reduce these risks.

Conclusion

To secure digital transactions and promote confidence in decentralized platforms, blockchain-based financial systems' integration of encryption and artificial intelligence (AI) is a significant breakthrough. For a long time, cryptography has been the foundation of blockchain security, which offers tools for secrecy, authentication, and data integrity. However, conventional cryptography techniques face severe limits as blockchain applications develop further and the threat environment becomes more complex. AI is a valuable addition to cryptography in tackling these issues because of its capacity to evaluate enormous datasets, identify irregularities instantly, and adjust to new threats.

This research has shown how AI and cryptography may work together to improve key management, streamline financial procedures, and strengthen blockchain security. AI-driven solutions like anomaly detection, predictive analytics, and real-time transaction monitoring significantly increase the efficacy of cryptographic systems, making them more dynamic and sensitive to changing threats. Additionally, AI helps to optimize consensus processes, guaranteeing quicker and more effective transaction validation—a critical component of expanding blockchain networks in the financial industry.

The combination of AI with encryption has promise, but drawbacks include the necessity for changing legislative frameworks, computational complexity, and possible biases in AI models. Policymakers, tech companies, and financial institutions must work together to develop safe, scalable, and transparent platforms that satisfy security and regulatory requirements to reap the benefits of this convergence fully.

To sum up, incorporating AI into blockchain cryptography systems holds great promise for improving financial systems' security, effectiveness, and scalability. As these technologies develop, their combined capabilities will significantly influence the future of safe and reliable blockchain transactions in the financial industry.

References

Abdullah, R. S., Faizal, M. A. (2018). Block Chain: Cryptographic Method in Fourth Industrial Revolution. *International Journal of Computer Network and Information Security*, *10*(11), 9. https://doi.org/10.5815/ijcnis.2018.11.02

Ahmmed, S., Narsina, D., Addimulam, S., & Boinapalli, N. R. (2021). AI-Powered Financial Engineering: Optimizing Risk Management and Investment Strategies. Asian Accounting and Auditing Advancement, 12(1), 37–45. https://4ajournal.com/article/view/96

Allam, A. R. (2020). Integrating Convolutional Neural Networks and Reinforcement Learning for Robotics Autonomy. *NEXG AI Review of America*, *1*(1), 101-118.

Boinapalli, N. R. (2020). Digital Transformation in U.S. Industries: AI as a Catalyst for Sustainable Growth. *NEXG AI Review of America*, *1*(1), 70-84.

Deming, C., Pasam, P., Allam, A. R., Mohammed, R., Venkata, S. G. N., & Kothapalli, K. R. V. (2021). Real-Time Scheduling for Energy Optimization: Smart Grid Integration with Renewable Energy. *Asia Pacific Journal of Energy and Environment*, *8*(2), 77-88. https://doi.org/10.18034/apjee.v8i2.762

Devarapu, K. (2020). Blockchain-Driven AI Solutions for Medical Imaging and Diagnosis in Healthcare. *Technology & Management Review*, *5*, 80-91. https://upright.pub/index.php/tmr/article/view/165

Devarapu, K. (2021). Advancing Deep Neural Networks: Optimization Techniques for Large-Scale Data Processing. *NEXG AI Review of America*, *2*(1), 47-61.

Devarapu, K., Rahman, K., Kamisetty, A., & Narsina, D. (2019). MLOps-Driven Solutions for Real-Time Monitoring of Obesity and Its Impact on Heart Disease Risk: Enhancing Predictive Accuracy in Healthcare. *International Journal of Reciprocal Symmetry and Theoretical Physics*, *6*, 43-55. https://upright.pub/index.php/ijrstp/article/view/160

Gade, P. K. (2019). MLOps Pipelines for GenAI in Renewable Energy: Enhancing Environmental Efficiency and Innovation. *Asia Pacific Journal of Energy and Environment*, *6*(2), 113-122. https://doi.org/10.18034/apjee.v6i2.776

Gade, P. K., Sridharlakshmi, N. R. B., Allam, A. R., & Koehler, S. (2021). Machine Learning-Enhanced Beamforming with Smart Antennas in Wireless Networks. *ABC Journal of Advanced Research*, *10*(2), 207-220. https://doi.org/10.18034/abcjar.v10i2.770

Gummadi, J. C. S., Narsina, D., Karanam, R. K., Kamisetty, A., Talla, R. R., & Rodriguez, M. (2020). Corporate Governance in the Age of Artificial Intelligence: Balancing Innovation with Ethical Responsibility. *Technology & Management Review*, *5*, 66-79. https://upright.pub/index.php/tmr/article/view/157

Gummadi, J. C. S., Thompson, C. R., Boinapalli, N. R., Talla, R. R., & Narsina, D. (2021). Robotics and Algorithmic Trading: A New Era in Stock Market Trend Analysis. *Global Disclosure of Economics and Business*, *10*(2), 129-140. https://doi.org/10.18034/gdeb.v10i2.769

Gurtu, A., Johny, J. (2019). Potential of Blockchain Technology in Supply Chain Management: A Literature Review. *International Journal of Physical Distribution & Logistics Management*, *49*(9), 881-900. https://doi.org/10.1108/IJPDLM-11-2018-0371

Justinia, T. (2019). Blockchain Technologies: Opportunities for Solving Real-World Problems in Healthcare and Biomedical Sciences. *Acta Informatica Medica*, *27*(4), 284-291. https://doi.org/10.5455/aim.2019.27.284-291

Kamisetty, A., Onteddu, A. R., Kundavaram, R. R., Gummadi, J. C. S., Kothapalli, S., Nizamuddin, M. (2021). Deep Learning for Fraud Detection in Bitcoin Transactions: An Artificial Intelligence-Based Strategy. *NEXG AI Review of America*, *2*(1), 32-46.

Karanam, R. K., Natakam, V. M., Boinapalli, N. R., Sridharlakshmi, N. R. B., Allam, A. R., Gade, P. K., Venkata, S. G. N., Kommineni,

H. P., & Manikyala, A. (2018). Neural Networks in Algorithmic Trading for Financial Markets. *Asian Accounting and Auditing Advancement*, *9*(1), 115–126. https://4ajournal.com/article/view/95

Kommineni, H. P. (2019). Cognitive Edge Computing: Machine Learning Strategies for IoT Data Management. *Asian Journal of Applied Science and Engineering*, *8*(1), 97-108. https://doi.org/10.18034/ajase.v8i1.123

Kommineni, H. P. (2020). Automating SAP GTS Compliance through AI-Powered Reciprocal Symmetry Models. *International Journal of Reciprocal Symmetry and Theoretical Physics*, *7*, 44-56. https://upright.pub/index.php/ijrstp/article/view/162

Kommineni, H. P., Fadziso, T., Gade, P. K., Venkata, S. S. M. G. N., & Manikyala, A. (2020). Quantifying Cybersecurity Investment Returns Using Risk Management Indicators. Asian Accounting and Auditing Advancement, 11(1), 117–128. Retrieved from https://4ajournal.com/article/view/97

Kothapalli, S. (2021). Blockchain Solutions for Data Privacy in HRM: Addressing Security Challenges. *Journal of Fareast International University*, *4*(1), 17-25. https://jfiu.weebly.com/uploads/1/4/9/0/149099275/2021_3.pdf

Kothapalli, S., Manikyala, A., Kommineni, H. P., Venkata, S. G. N., Gade, P. K., Allam, A. R., Sridharlakshmi, N. R. B., Boinapalli, N. R., Onteddu, A. R., & Kundavaram, R. R. (2019). Code Refactoring Strategies for DevOps: Improving Software Maintainability and Scalability. *ABC Research Alert*, *7*(3), 193–204. https://doi.org/10.18034/ra.v7i3.663

Kundavaram, R. R., Rahman, K., Devarapu, K., Narsina, D., Kamisetty, A., Gummadi, J. C. S., Talla, R. R., Onteddu, A. R., & Kothapalli, S. (2018). Predictive Analytics and Generative AI for Optimizing Cervical and Breast Cancer Outcomes: A Data-Centric Approach. *ABC Research Alert*, *6*(3), 214-223. https://doi.org/10.18034/ra.v6i3.672

Makridakis, S., Christodoulou, K. (2019). Blockchain: Current Challenges and Future Prospects/Applications. *Future Internet*, *11*(12), 258. https://doi.org/10.3390/fi11120258

Manikyala, A. (2022). Sentiment Analysis in IoT Data Streams: An NLP-Based Strategy for Understanding Customer Responses. *Silicon Valley Tech Review*, *1*(1), 35-47.

Narsina, D. (2020). The Integration of Cybersecurity, IoT, and Fintech: Establishing a Secure Future for Digital Banking. *NEXG AI Review of America*, *1*(1), 119-134. https://nexgaireview.weebly.com/uploads/9/9/8/2/9982776/2020.8.pdf

Narsina, D., Devarapu, K., Kamisetty, A., Gummadi, J. C. S., Richardson, N., & Manikyala, A. (2021). Emerging Challenges in Mechanical Systems: Leveraging Data Visualization for Predictive Maintenance. *Asian Journal of Applied Science and Engineering*, *10*(1), 77-86. https://doi.org/10.18034/ajase.v10i1.124

Narsina, D., Gummadi, J. C. S., Venkata, S. S. M. G. N., Manikyala, A., Kothapalli, S., Devarapu, K., Rodriguez, M., & Talla, R. R. (2019). AI-Driven Database Systems in FinTech: Enhancing Fraud Detection and Transaction Efficiency. *Asian Accounting and Auditing Advancement*, *10*(1), 81–92. https://4ajournal.com/article/view/98

Niranjanamurthy, M., Nithya, B. N., Jagannatha, S. (2019). Analysis of Blockchain Technology: Pros, Cons and SWOT. *Cluster Computing, suppl. 6*, *22*, 14743-14757. https://doi.org/10.1007/s10586-018-2387-5

Onteddu, A. R., Rahman, K., Roberts, C., Kundavaram, R. R., Kothapalli, S. (2022). Blockchain-Enhanced Machine Learning for Predictive Analytics in Precision Medicine. *Silicon Valley Tech Review*, *1*(1), 48-60. https://www.siliconvalley.onl/uploads/9/9/8/2/9982776/2022.4

Onteddu, A. R., Venkata, S. S. M. G. N., Ying, D., & Kundavaram, R. R. (2020). Integrating Blockchain Technology in FinTech Database Systems: A Security and Performance Analysis. Asian Accounting and Auditing Advancement, 11(1), 129–142. https://4ajournal.com/article/view/99

Ravindran, S. (2019). Blockchain and Building Information Modeling (BIM): Review and Applications in Post-Disaster Recovery. *Buildings*, *9*(6), 149. https://doi.org/10.3390/buildings9060149

Richardson, N., Manikyala, A., Gade, P. K., Venkata, S. S. M. G. N., Asadullah, A. B. M., & Kommineni, H. P. (2021). Emergency Response Planning: Leveraging Machine Learning for Real-Time Decision-Making. *Technology & Management Review*, *6*, 50-62. https://upright.pub/index.php/tmr/article/view/163

Roberts, C., Kundavaram, R. R., Onteddu, A. R., Kothapalli, S., Tuli, F. A., Miah, M. S. (2020). Chatbots and Virtual Assistants in HRM: Exploring Their Role in Employee Engagement and Support. *NEXG AI Review of America*, *1*(1), 16-31.

Rodriguez, M., Mohammed, M. A., Mohammed, R., Pasam, P., Karanam, R. K., Vennapusa, S. C. R., & Boinapalli, N. R. (2019). Oracle EBS and Digital Transformation: Aligning Technology with Business Goals. *Technology & Management Review*, *4*, 49-63. https://upright.pub/index.php/tmr/article/view/151

Rodriguez, M., Sridharlakshmi, N. R. B., Boinapalli, N. R., Allam, A. R., & Devarapu, K. (2020). Applying Convolutional Neural Networks for IoT Image Recognition. *International Journal of Reciprocal Symmetry and Theoretical Physics*, *7*, 32-43. https://upright.pub/index.php/ijrstp/article/view/158

Sgantzos, K., Grigg, I. (2019). Artificial Intelligence Implementations on the Blockchain. Use Cases and Future Applications. *Future Internet*, *11*(8), 170. https://doi.org/10.3390/fi11080170

Song, R., Song, Y., Liu, Z., Tang, M., Zhou, K. (2019). GaiaWorld: A Novel Blockchain System Based on Competitive PoS Consensus Mechanism. *Computers, Materials, & Continua*, *60*(3), 973-987. https://doi.org/10.32604/cmc.2019.06035

Sridharlakshmi, N. R. B. (2020). The Impact of Machine Learning on Multilingual Communication and Translation Automation. *NEXG AI Review of America*, *1*(1), 85-100.

Sridharlakshmi, N. R. B. (2021). Data Analytics for Energy-Efficient Code Refactoring in Large-Scale Distributed

Systems. *Asia Pacific Journal of Energy and Environment*, *8*(2), 89-98. https://doi.org/10.18034/apjee.v8i2.771

Talla, R. R., Manikyala, A., Gade, P. K., Kommineni, H. P., & Deming, C. (2022). Leveraging AI in SAP GTS for Enhanced Trade Compliance and Reciprocal Symmetry Analysis. *International Journal of Reciprocal Symmetry and Theoretical Physics*, *9*, 10-23. https://upright.pub/index.php/ijrstp/article/view/164

Talla, R. R., Manikyala, A., Nizamuddin, M., Kommineni, H. P., Kothapalli, S., Kamisetty, A. (2021). Intelligent Threat Identification System: Implementing Multi-Layer Security Networks in Cloud Environments. NEXG AI Review of America, 2(1), 17-31.

Talla, R. R., Manikyala, A., Nizamuddin, M., Kommineni, H. P., Kothapalli, S., Kamisetty, A. (2021). Intelligent Threat Identification System: Implementing Multi-Layer Security Networks in Cloud Environments. NEXG AI Review of America, 2(1), 17-31. https://nexgaireview.weebly.com/uploads/9/9/8/2/9982776/2021.2.pdf

Talla, R. R., Manikyala, A., Nizamuddin, M., Kommineni, H. P., Kothapalli, S., Kamisetty, A. (2021). Intelligent Threat Identification System: Implementing Multi-Layer Security Networks in Cloud Environments. NEXG AI Review of America, 2(1), 17-31.

Thompson, C. R., Talla, R. R., Gummadi, J. C. S., Kamisetty, A (2019). Reinforcement Learning Techniques for Autonomous Robotics. *Asian Journal of Applied Science and Engineering*, *8*(1), 85-96. https://ajase.net/article/view/94

Venkata, S. S. M. G. N., Gade, P. K., Kommineni, H. P., Manikyala, A., & Boinapalli , N. R. (2022). Bridging UX and Robotics: Designing Intuitive Robotic Interfaces. *Digitalization & Sustainability Review*, 2(1), 43-56. https://upright.pub/index.php/dsr/article/view/159

Xiao-Ling, J., Zhang, M., Zhou, Z., Yu, X. (2019). Application of a Blockchain Platform to Manage and Secure Personal Genomic Data: A Case Study of LifeCODE.ai in China. *Journal of Medical Internet Research*, *21*(9). https://doi.org/10.2196/13587

Zheng, X-l., Zhu, M-y., Li, Q-b., Chen, C-c., Tan, Y-c. (2019). FinBrain: When Finance Meets AI 2.0. *Frontiers of Information Technology & Electronic Engineering*, *20*(7), 914-924. https://doi.org/10.1631/FITEE.1700822

--0--

How to cite this article

Nizamuddin, M., Devarapu, K., Onteddu, A. R., & Kundavaram, R. R. (2022). Cryptography Converges with AI in Financial Systems: Safeguarding Blockchain Transactions with AI. *Asian Business Review*, *12*(3), 97-106. https://doi.org/10.18034/abr.v12i3.742