International Journal of
Digital Futures and Innovation
VOL. 01 | No. 1 | 2026
P-ISSN: XXXXXXXXX | E-ISSN: XXXXXXXXX

BLOCKCHAIN TECHNOLOGY ENHANCING SECURITY IN DIGITAL FINANCIAL SYSTEMS

Rania Zara
BS Clinical Psychology, (CCP), Center for Clinical Psychology, University of the Punjab, Lahore, Pakistan

ABSTRACT

Blockchain technology has emerged as an innovative technological solution for improving security, transparency, reliability, and trust in digital financial systems. The rapid expansion of online banking, electronic payments, digital currencies, financial technology platforms, and internet-based transactions has increased the need for advanced security mechanisms to protect financial information and prevent cybercrime. Traditional financial systems frequently depend on centralized databases and intermediaries, which may create vulnerabilities associated with unauthorized access, data manipulation, identity theft, financial fraud, and cyberattacks. Blockchain technology offers an alternative approach through decentralized data storage, cryptographic protection, distributed consensus mechanisms, and immutable transaction records. These characteristics can strengthen financial security by improving transaction verification, reducing opportunities for unauthorized modification, and increasing transparency in financial activities. This research examines the role of blockchain technology in enhancing security in digital financial systems, particularly in online banking, electronic payments, international transactions, smart contracts, digital identity management, and decentralized finance. The study adopts a qualitative literature-based methodology and reviews recent academic publications and research reports published between 2023 and 2025. It investigates the security benefits, technological applications, implementation challenges, and future opportunities associated with blockchain integration. The findings indicate that blockchain can strengthen transaction integrity, improve traceability, support secure information sharing, and reduce certain risks associated with centralized financial infrastructures. However, challenges involving scalability, regulatory uncertainty, privacy protection, smart contract vulnerabilities, interoperability, and implementation costs remain significant. The research concludes that blockchain technology has considerable potential to improve digital financial security when supported by effective governance, strong cybersecurity practices, regulatory compliance, and appropriate technological infrastructure.

KEYWORDS:*Blockchain Technology, Digital Financial Systems, Financial Security, Cybersecurity, Financial Transactions, Cryptography, Decentralization, Distributed Ledger Technology, Smart Contracts, Digital Banking, Financial Fraud Prevention, Data Integrity, Digital Payments, Decentralized Finance, Information Security.*

INTRODUCTION

The financial industry has experienced substantial transformation because of the rapid development of digital technologies and internet-based financial services. Traditional financial activities that previously depended on physical banking branches, paper-based documentation, and manual transaction processing are increasingly conducted through online banking platforms, mobile applications, electronic payment systems, and digital financial networks. Weerawarna, R., Miah, S. J., & Shao, X. (2023). found that These developments have improved the speed, convenience, and accessibility of financial services for individuals, businesses, and institutions. Customers can transfer money, pay bills, manage accounts, and conduct financial transactions without visiting physical banking institutions. However, the growing dependence on digital financial infrastructure has also increased exposure to cybersecurity threats, including identity theft, phishing, unauthorized account access, data breaches, and financial fraud. Consequently, financial institutions require reliable security technologies capable of protecting sensitive information and maintaining confidence in

International Journal of
Digital Futures and Innovation
VOL. 01 | No. 1 | 2026
P-ISSN: XXXXXXXXX | E-ISSN: XXXXXXXXX

digital transactions.Blockchain technology has attracted considerable attention as a potential solution to security challenges in digital financial systems. Blockchain is a form of distributed ledger technology that records transactions across a network of participating computers. Instead of maintaining transaction information exclusively within a single centralized database, blockchain distributes records across multiple network participants according to an established consensus mechanism. Transactions are organized into blocks that are cryptographically linked, creating a chronological record of financial activities. The use of cryptographic techniques, digital signatures, and consensus protocols helps protect transaction integrity and makes unauthorized modification more difficult. These characteristics provide opportunities for improving financial transparency, reducing dependence on certain intermediaries, and strengthening trust among participants. According to Wu et al. (2024), blockchain has important applications in financial services, particularly in securities trading, transaction verification, and distributed financial operations.

Cybersecurity is a fundamental requirement for modern financial systems because financial institutions process sensitive customer information and valuable monetary transactions. Traditional centralized systems may become attractive targets for cybercriminals because compromising a central database or critical administrative account can expose substantial amounts of information. Blockchain offers a different security architecture through distributed records, cryptographic verification, and shared transaction validation. These features can improve the integrity and traceability of financial records and make certain types of unauthorized manipulation more difficult. Ali Eyadat et al. (2025) examined the influence of blockchain technology on reducing cybersecurity risks in commercial bank financial transactions, highlighting its potential contribution to financial security. Nevertheless, blockchain should not be understood as a complete cybersecurity solution because external applications, user accounts, digital wallets, and connected systems can remain vulnerable to attacks.Blockchain technology has several potential applications in digital banking and financial services. Financial institutions can explore its use in payment processing, transaction settlement, international money transfers, digital identity management, securities trading, and financial recordkeeping. Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Explained that Smart contracts can automate predefined financial operations when specified conditions are satisfied, potentially reducing manual processing and improving transaction transparency. Blockchain-based payment systems may also improve the traceability of financial transfers by maintaining verifiable transaction histories. Daah et al. (2024) proposed integrating blockchain with Zero Trust security models in the financial industry, demonstrating how distributed ledger technology can contribute to a broader security architecture. Such applications indicate that blockchain may support the modernization of financial infrastructure when appropriately integrated with existing banking systems.

Despite its potential benefits, blockchain implementation in digital financial systems presents several technological, operational, and regulatory challenges. Public blockchain networks may experience scalability limitations, transaction delays, and fluctuating transaction costs when network activity increases. Permissioned blockchain networks can offer greater institutional control, but they require governance arrangements and trusted participation among authorized organizations. Smart contracts may also contain programming errors or design weaknesses that could result in financial losses. Privacy is another important concern because transparent transaction records may expose sensitive financial information if systems are not designed with appropriate confidentiality protections. Regulatory uncertainty,

International Journal of
Digital Futures and Innovation
VOL. 01 | No. 1 | 2026
P-ISSN: XXXXXXXXX | E-ISSN: XXXXXXXXX

interoperability limitations, implementation costs, and shortages of specialized technical expertise can further restrict adoption. Financial institutions must therefore evaluate both the advantages and limitations of blockchain before incorporating it into critical financial operations.The purpose of this research is to investigate how blockchain technology can enhance security in digital financial systems and contribute to the development of more reliable financial services. The study examines the technological characteristics of blockchain, its applications in digital banking and financial transactions, and its potential to improve data integrity, transaction transparency, fraud prevention, and cybersecurity. It also explores the challenges associated with blockchain adoption, including privacy, scalability, regulatory compliance, smart contract security, and institutional readiness. The research is significant because financial institutions increasingly require innovative technologies to protect digital transactions and maintain customer confidence. By examining academic literature published between 2023 and 2025, the study aims to provide a comprehensive understanding of blockchain's security contributions and identify recommendations for its responsible implementation in modern financial infrastructures.

RESEARCH QUESTION

1. How does blockchain technology enhance security in digital financial systems, particularly in relation to transaction integrity, data protection, financial fraud prevention, transparency, and cybersecurity, and what challenges influence its successful implementation?

RESEARCH OBJECTIVES

1. To examine the role of blockchain technology in enhancing security within digital financial systems.

LITERATURE REVIEW

Blockchain technology has developed into an important area of research within the financial technology industry because of its potential to improve the security, transparency, and efficiency of financial transactions. Digital financial systems depend on the accurate processing, storage, and exchange of sensitive financial information. Traditional financial infrastructure commonly relies on centralized databases and trusted intermediaries to validate transactions and maintain records. Sharma, G. D., Tiwari, A. K., Chopra, R., & Dev, D. (2024). Explains that Although these arrangements have supported financial operations for many years, they may create security risks associated with centralized access, information manipulation, and single points of failure. Blockchain introduces a distributed approach in which transaction records are maintained across a network of participating computers. This architecture can reduce dependence on a single recordkeeping authority and provide a shared, verifiable history of financial transactions.Weerawarna et al. (2023), in their research on emerging advances of blockchain technology in finance, examined the development of blockchain-based financial systems and identified important opportunities and challenges associated with their adoption. Their research highlights the growing importance of blockchain as a financial information technology and discusses its possible contribution to transforming financial services. The study also recognizes that the practical implementation

International Journal of
Digital Futures and Innovation
VOL. 01 | No. 1 | 2026
P-ISSN: XXXXXXXXX | E-ISSN: XXXXXXXXX

of blockchain remains influenced by technical limitations, organizational requirements, and the development of appropriate standards. These observations demonstrate that blockchain should be understood not simply as a digital currency technology but as an infrastructure capable of supporting different financial operations.Blockchain's relevance to digital finance is based on several interconnected characteristics. Decentralization distributes transaction records across participating network members, cryptography helps protect information, and consensus mechanisms provide procedures for validating transactions. Once transactions are confirmed and added to a blockchain, altering historical records generally requires overcoming substantial network and cryptographic protections. However, the strength of these protections depends on the blockchain's architecture, governance, implementation, and operating environment. Financial institutions must therefore evaluate the specific characteristics of each blockchain platform before using it to support important financial services.

Blockchain architecture plays an important role in determining how financial information is stored, verified, and protected. A blockchain generally consists of connected blocks containing transaction data and cryptographic information that links each block to the preceding one. The distributed nature of the network allows participating nodes to maintain and verify records according to established protocols. This structure creates an auditable transaction history and makes unauthorized historical modification more difficult than in many conventional recordkeeping arrangements.Cryptographic hashing is an important component of blockchain security. A cryptographic hash function converts input information into a fixed-length output that changes significantly when the original information is modified. Blockchain systems use hashes to connect blocks and help identify changes in recorded information. Digital signatures also support financial security by allowing transaction participants to demonstrate control over cryptographic credentials and authorize transactions. These mechanisms contribute to transaction authenticity and integrity.Luo et al. (2024), in their survey of blockchain applications in cryptographic protocols, discussed the role of blockchain in improving security, authentication, and data integrity. Their research demonstrates that blockchain can support security-related applications through decentralization, traceability, and cryptographic verification. Such characteristics are relevant to financial services because transactions require reliable identification, authentication, and verification procedures.However, blockchain cryptography does not automatically protect every component of a financial application. The security of a financial platform also depends on the protection of private keys, endpoint devices, software interfaces, and account-management systems.

Decentralization is one of the most important characteristics distinguishing blockchain from traditional centralized financial databases. In conventional financial systems, transaction information may be stored and managed by a central organization. This arrangement can simplify administration and regulatory supervision, but it can also create a concentrated target for cyberattacks. If an attacker compromises a central database or privileged account, the consequences may affect a large number of users and financial records.Blockchain distributes transaction records across participating nodes, allowing the network to maintain a shared record of financial activity. This arrangement can improve resilience because the failure or compromise of one participating node does not necessarily result in the loss of the entire transaction history. Consensus mechanisms also help participants agree on valid transactions and maintain consistency across distributed records.Karadag et al. (2024), in their systematic literature review of blockchain in finance, examined the technical features, benefits,

International Journal of
Digital Futures and Innovation
VOL. 01 | No. 1 | 2026
P-ISSN: XXXXXXXXX | E-ISSN: XXXXXXXXX

challenges, and financial applications of blockchain. Their research identifies improvements in transparency, efficiency, and security as important potential benefits. The review also indicates that the choice between public and permissioned blockchain systems has important implications for financial institutions.Public blockchain networks generally allow broader participation, while permissioned networks restrict access to approved participants. Financial institutions may prefer permissioned systems when they require controlled access, identifiable participants, and governance arrangements that align with regulatory obligations. However, permissioned networks also introduce questions about the distribution of authority and the independence of network participants. The appropriate architecture therefore depends on the financial institution's operational requirements, threat environment, and regulatory responsibilities.Cryptographic mechanisms are essential for protecting information and maintaining the integrity of digital financial transactions. Blockchain uses cryptographic techniques to support transaction authentication, protect records from unauthorized modification, and establish relationships between blocks. Digital signatures allow transactions to be associated with the relevant cryptographic credentials, while hash functions provide mechanisms for detecting changes to recorded data.

In digital banking, transaction integrity is particularly important because financial institutions must ensure that payment instructions, account records, and settlement information remain accurate. Unauthorized changes to financial records can create substantial economic losses and undermine customer confidence. Blockchain-based recordkeeping may strengthen the ability of institutions to verify transaction histories and identify inconsistencies.Wu et al. (2024) explain that blockchain's consensus-based verification and distributed trust can support financial applications by reducing reliance on conventional third-party verification arrangements. Their survey also examines financial blockchain platforms and their applications in securities-related activities. The research demonstrates that blockchain's cryptographic and distributed architecture offers opportunities to improve the authenticity and traceability of financial transactions.Nevertheless, cryptographic security has limitations. The protection of blockchain records does not necessarily guarantee the confidentiality of transaction information. Depending on the blockchain design, transaction metadata and financial relationships may remain visible to network participants. Financial institutions must therefore consider privacy-preserving mechanisms, access controls, and appropriate data-management practices alongside cryptographic verification.Digital banking has become increasingly important because customers expect financial services to be available through mobile applications, internet platforms, and electronic payment systems. Banks must manage substantial volumes of financial transactions while protecting customer accounts, transaction records, and personal information. Wu, H., Yao, Q., Liu, Z., Huang, B., Zhuang, Y., Tang, H., & Liu, E. (2024). revealed that Blockchain may contribute to the modernization of banking infrastructure by supporting distributed recordkeeping, transaction verification, and secure information exchange.

Ehsan et al. (2025) examined blockchain-based cybersecurity solutions for secure financial transactions in digital banking systems. Their research discusses blockchain's potential role in addressing financial security threats such as unauthorized access, fraud, and data breaches. Similarly, Ali Eyadat et al. (2025) investigated blockchain's influence on cybersecurity risks in commercial bank financial transactions. These studies support the importance of examining blockchain as part of a wider financial security strategy.Despite these opportunities, banks cannot rely exclusively on blockchain to protect customer accounts.

International Journal of
Digital Futures and Innovation
VOL. 01 | No. 1 | 2026
P-ISSN: XXXXXXXXX | E-ISSN: XXXXXXXXX

Authentication systems, secure devices, monitoring procedures, regulatory controls, and incident-response capabilities remain essential. Blockchain can improve the reliability of shared financial records, but institutions must continue protecting the applications and infrastructure through which customers access banking services.Electronic payment systems have transformed the movement of money by allowing individuals and businesses to transfer funds through digital platforms. However, international financial transfers may involve multiple institutions, settlement processes, intermediaries, and compliance requirements. These arrangements can create delays, administrative costs, and difficulties in tracking transaction information.Blockchain has attracted attention as a potential infrastructure for improving payment processing and international settlement. Distributed ledgers can allow authorized participants to access shared transaction records and verify payment activities. Smart contracts may also support predefined payment conditions and automated settlement processes. These capabilities could improve operational efficiency and reduce certain reconciliation problems.Sharma et al. (2024), in their research on the past, present, and future of blockchain in finance, examined the development of blockchain applications and their potential influence on financial services. Their systematic review illustrates how blockchain is being explored in different financial activities, including securities trading and investment-related operations.

However, blockchain-based payment systems still face challenges involving transaction throughput, settlement finality, exchange-rate exposure, legal compliance, and interoperability with traditional payment networks. The security of international payment applications also depends on how financial institutions manage customer identities, transaction monitoring, and cross-border regulatory obligations. Blockchain may improve particular stages of payment processing, but its practical benefits must be evaluated against the requirements of existing financial infrastructure.Smart contracts are computer programs deployed on blockchain networks that execute predefined operations when specified conditions are satisfied. They can support automated financial processes, including payment execution, settlement procedures, digital asset transfers, and certain lending activities. By reducing dependence on manual transaction processing, smart contracts may improve operational efficiency and provide a transparent record of automated actions.In digital financial systems, smart contracts can help ensure that particular transactions follow predetermined rules. Karadag, B., Zaim, A. H., & Akbulut, A. (2024). Elaborated on For example, a financial agreement may specify that a payment is processed only after a particular condition has been verified. This may reduce certain administrative errors and improve the consistency of transaction execution.Wu et al. (2024) discuss smart contracts as an important component of blockchain-based financial platforms and describe their relevance to securities trading and other financial applications. Their research highlights the importance of examining the functionality and security characteristics of blockchain platforms before using them in financial operations.Despite their advantages, smart contracts introduce security risks because software errors may produce unexpected outcomes.

METHODOLOGY

The present study adopts a qualitative, literature-based research methodology to investigate the role of blockchain technology in enhancing security in digital financial systems. The research is based on the examination, interpretation, and synthesis of academic publications, systematic literature reviews, research articles, and relevant institutional reports published

International Journal of
Digital Futures and Innovation
VOL. 01 | No. 1 | 2026
P-ISSN: XXXXXXXXX | E-ISSN: XXXXXXXXX

between 2023 and 2025. The literature focuses on blockchain architecture, cryptographic security, distributed ledger technology, digital banking, electronic payments, smart contracts, digital identity management, decentralized finance, financial fraud prevention, and cybersecurity. Relevant publications were identified through scholarly research platforms and academic databases, including Google Scholar, SpringerLink, ScienceDirect, Wiley Online Library, IEEE Xplore, MDPI, and other recognized research sources. The selection of literature was guided by its relevance to the research question and objectives, publication period, academic credibility, and contribution to understanding blockchain-based financial security. Particular attention was given to studies examining the security characteristics of blockchain, its financial applications, and the technological and regulatory challenges associated with implementation. The selected literature was reviewed to identify recurring themes, compare different research perspectives, and understand how blockchain may address vulnerabilities in conventional financial infrastructure. The research also examines the relationship between blockchain technology and other cybersecurity approaches, including cryptographic authentication, access control, Zero Trust security, and transaction monitoring. A qualitative methodology was considered appropriate because the purpose of the study is to explore the broader technological and institutional implications of blockchain rather than measure the performance of a specific blockchain network through an independent experiment. The research does not involve primary data collection through questionnaires, interviews, or direct banking-system testing. Instead, it uses secondary information from existing academic research to develop an integrated understanding of the subject.

RESEARCH DESIGN

This study follows a descriptive and exploratory qualitative research design based on a structured review and thematic analysis of secondary academic literature. The descriptive component examines the fundamental characteristics of blockchain technology and explains how decentralization, cryptographic protection, consensus mechanisms, distributed ledgers, and smart contracts contribute to financial security. The exploratory component investigates the potential applications of blockchain in digital banking, electronic payment processing, international financial transfers, identity management, financial recordkeeping, and decentralized finance. The research design is organized according to the main research question and research objectives to ensure that the investigation addresses the technological, financial, operational, and regulatory dimensions of blockchain adoption. The research process involves identifying relevant publications, examining their research purposes and findings, grouping similar concepts into themes, comparing different perspectives, and developing an overall interpretation of the available evidence. The literature published between 2023 and 2025 is prioritized to reflect recent developments in blockchain-based financial systems and cybersecurity. The study considers several major analytical dimensions, including transaction integrity, data confidentiality, authentication, fraud prevention, transparency, system reliability, scalability, and institutional governance. It also distinguishes between public and permissioned blockchain systems because their access arrangements and governance structures may influence their suitability for financial institutions. The design recognizes that blockchain security cannot be evaluated exclusively through technological characteristics because successful implementation also depends on organizational readiness, regulatory requirements, employee expertise, and integration with existing financial

International Journal of
Digital Futures and Innovation
VOL. 01 | No. 1 | 2026
P-ISSN: XXXXXXXXX | E-ISSN: XXXXXXXXX

infrastructure. Consequently, the study examines blockchain as part of a broader financial cybersecurity environment rather than as an independent security solution.

DATA ANALYSIS

The data analysis process is based on qualitative thematic analysis of the selected academic publications and institutional research materials. The reviewed literature was examined to identify recurring concepts, research findings, technological applications, security advantages, and implementation challenges associated with blockchain in digital financial systems. The analysis began with familiarization with the selected publications, followed by the identification of information relevant to the research question and objectives. Similar findings were organized into major themes to provide a systematic understanding of blockchain's security contributions. The first theme focused on cryptographic protection and transaction integrity, examining how hashing, digital signatures, and cryptographic verification can support the authenticity and reliability of financial records. The second theme examined decentralization and distributed ledger technology, particularly their potential to reduce dependence on centralized databases and improve the resilience of transaction-recording systems. The third theme concerned the application of blockchain in digital banking, electronic payments, international transfers, and securities transactions. The fourth theme focused on smart contracts and their ability to automate predefined financial processes while introducing additional software-related security considerations. The fifth theme examined fraud prevention, digital identity management, and transaction traceability, with particular attention to how blockchain can complement conventional cybersecurity mechanisms. The sixth theme focused on privacy protection, regulatory compliance, scalability, interoperability, and implementation costs. After identifying these themes, the findings of different publications were compared to determine areas of agreement, differences, and emerging research gaps. For example, several studies identify blockchain's potential to strengthen transparency and transaction integrity, while also recognizing that the security of external applications and user credentials remains a significant concern..

FINDINGS

The findings of this literature-based study indicate that blockchain technology has considerable potential to strengthen security in digital financial systems through its distributed architecture, cryptographic mechanisms, transaction transparency, and shared verification processes. The reviewed literature suggests that blockchain can improve transaction integrity by maintaining cryptographically connected records that are difficult to modify without detection. This characteristic may help financial institutions maintain reliable transaction histories and improve accountability in financial operations. Another important finding concerns decentralization, which can reduce dependence on a single centralized recordkeeping system and improve the resilience of certain financial infrastructures. The literature also identifies blockchain's potential applications in digital banking, electronic payments, international transfers, securities trading, and financial record management. Smart contracts represent another significant application because they can automate predefined financial operations and provide verifiable records of executed transactions. Research by Wu et al. (2024), Karadag et al. (2024), and Sharma et al. (2024) demonstrates the expanding role of blockchain in financial services and identifies security, transparency, and operational efficiency as important areas of interest. The findings also indicate that blockchain may

International Journal of
Digital Futures and Innovation
VOL. 01 | No. 1 | 2026
P-ISSN: XXXXXXXXX | E-ISSN: XXXXXXXXX

support financial fraud investigations by improving transaction traceability and providing verifiable records of financial activity. Ali Eyadat et al. (2025) specifically examine the relationship between blockchain and cybersecurity risks in commercial banking, while Ehsan et al. (2025) investigate blockchain-based cybersecurity solutions for digital banking transactions. Nevertheless, the analysis identifies important limitations that may affect blockchain adoption. Smart contract vulnerabilities, compromised private keys, insecure applications, privacy concerns, scalability limitations, and regulatory uncertainty can create additional risks. Blockchain also cannot automatically distinguish legitimate financial activity from fraudulent activity because a transaction may be technically valid while still being associated with deception or stolen credentials. Another significant finding is that the effectiveness of blockchain depends on the broader cybersecurity environment, including authentication procedures, access controls, security monitoring, governance, and institutional preparedness.

CONCLUSION

Blockchain technology represents an important development in the transformation of digital financial systems because it offers new approaches to improving transaction security, data integrity, transparency, and trust. The findings of this research demonstrate that blockchain's distributed architecture, cryptographic mechanisms, consensus protocols, and immutable transaction records can contribute to strengthening the security of modern financial operations. These characteristics provide opportunities to improve digital banking, electronic payments, international money transfers, securities trading, digital identity management, and financial recordkeeping. The research also highlights the potential of smart contracts to automate predefined financial processes and reduce certain operational risks associated with manual transaction processing. Furthermore, blockchain-based systems may support financial fraud investigations by providing verifiable transaction histories and improving the traceability of financial activities. However, the implementation of blockchain technology also presents several challenges that require careful consideration. Smart contract vulnerabilities, compromised private keys, data privacy concerns, scalability limitations, interoperability problems, regulatory uncertainty, and implementation costs may affect the reliability and adoption of blockchain-based financial services. The study emphasizes that blockchain cannot independently eliminate cybercrime or guarantee complete financial security because external applications, user devices, authentication systems, and institutional processes may remain vulnerable. Therefore, financial organizations should integrate blockchain with established cybersecurity practices, including encryption, secure identity verification, access control, continuous monitoring, and appropriate risk-management procedures. Governments and regulatory authorities should also develop clear guidelines to encourage responsible blockchain adoption while protecting financial consumers and maintaining institutional accountability. Financial institutions should invest in technical infrastructure, employee training, independent security assessments, and effective governance arrangements to ensure the reliability of blockchain-based services. Particular attention should be given to protecting customer information and maintaining compatibility between blockchain platforms and existing banking systems. Future research should investigate the practical performance of blockchain-based financial security solutions through empirical studies, experimental testing, and institutional case studies. In conclusion, blockchain technology has significant potential to enhance security in digital financial systems, but its

International Journal of
Digital Futures and Innovation
VOL. 01 | No. 1 | 2026
P-ISSN: XXXXXXXXX | E-ISSN: XXXXXXXXX

effectiveness depends on appropriate implementation, technological reliability, regulatory compliance, and continuous cybersecurity evaluation.

REFERENCES

Weerawarna, R., Miah, S. J., & Shao, X. (2023). Emerging advances of blockchain technology in finance: a content analysis. Personal and Ubiquitous Computing, 27(4), 1495-1508.

Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework. Electronics, 13(5), 865.

Sharma, G. D., Tiwari, A. K., Chopra, R., & Dev, D. (2024). Past, present, and future of block-chain in finance. Journal of Business Research, 177, 114640.

Wu, H., Yao, Q., Liu, Z., Huang, B., Zhuang, Y., Tang, H., & Liu, E. (2024). Blockchain for finance: A survey. IET blockchain, 4(2), 101-123.

Karadag, B., Zaim, A. H., & Akbulut, A. (2024). Blockchain in finance: A systematic literature review. Journal of Business Economics and Finance, 13(2), 113-129.