Journal of Engineering Science and Technology
Vol. 20, No. 3 (2025) 723 - 738


# ENHANCING TRUST IN DIGITAL FINANCE: BLOCKCHAIN AND AI FOR SECURE AND TRANSPARENT FINTECH SOLUTIONS

SENNY LUCKYARDI,
MUHAMAD FAHREZI*,EDDY SOERYANTO SOEGOTO

Universitas Komputer Indonesia, Indonesia
*Corresponding Author: fahrezi.21222225@mahasiswa.unikom.ac.id

**Abstract**

The rapid advancement of financial technology (FinTech) has brought significant innovations while raising concerns about security, transparency, and trust. This study explores how blockchain and artificial intelligence (AI) enhance trust in digital finance by strengthening security, improving fraud detection, and ensuring regulatory compliance. This study systematically reviews the integration of blockchain and AI in financial operations using a qualitative research approach. The findings indicate that blockchain enhances transaction security through decentralization and immutability, while AI significantly improves fraud detection and risk assessment through predictive analytics and machine learning. These advancements are driven by blockchain's ability to ensure data integrity and AI's capacity to analyse vast datasets in real time. This research highlights the potential of these technologies to boost consumer confidence, promote financial inclusion, and enhance the resilience of digital financial systems. However, regulatory complexities, high integration costs, and interoperability issues must be addressed to enable broader adoption.

Keywords: Artificial intelligence (AI), Blockchain, Digital finance, Fraud detection, Regulatory compliance.

## 1. Introduction

The rapid advancement of digital finance has reshaped the global financial landscape, providing businesses and consumers with greater accessibility, efficiency, and convenience [1, 2]. The rise of financial technology (FinTech) companies has introduced a new paradigm that challenges traditional banking by offering innovative solutions such as digital payments, peer-to-peer lending, decentralized finance (DeFi), and robo-advisors [3, 4]. These advancements have expanded access to financial services, reduced transaction costs, and improved financial inclusion. However, despite these benefits, the digital financial ecosystem faces significant challenges, including security risks, privacy concerns, regulatory compliance issues, and fraudulent activities.

Extensive reports highlight growing concerns in digital finance, particularly the increasing vulnerability of online transactions to cyber threats, identity theft, and financial fraud [3, 5, 6]. As financial activities are digitized, malicious actors continuously develop sophisticated methods to exploit security weaknesses. Traditional security measures-such as encryption, multi-factor authentication, and centralized regulatory oversight-provide a baseline level of protection but often fall short in addressing the rapidly evolving threat landscape [7, 8]. Moreover, digital finance heavily relies on centralized systems for transaction processing and data management, raising concerns about transparency, data integrity, and the risk of single points of failure [9, 10].

Transparency in financial transactions is another major challenge, as centralized institutions control data management, increasing the risks of data manipulation, insider fraud, and accountability gaps. In many cases, users have limited visibility into how their financial information is processed, stored, or shared, leading to trust issues in digital finance [10, 11]. At the same time, regulatory frameworks struggle to keep pace with the rapid evolution of digital finance, resulting in inconsistent compliance requirements across different jurisdictions. This regulatory disparity creates obstacles for FinTech firms seeking to expand globally while navigating diverse legal landscapes.

To address these critical challenges, emerging technologies such as blockchain and artificial intelligence (AI) are increasingly integrated into digital financial systems to enhance security, transparency, and efficiency [12, 13]. Blockchain technology significantly reduces fraud, unauthorized modifications, and single points of failure by providing a decentralized, immutable ledger that securely records transactions [14]. By leveraging cryptographic principles and consensus mechanisms, blockchain ensures that financial transactions remain verifiable, tamper-proof, and resistant to fraudulent activities. Its decentralized nature eliminates the need for intermediaries, fostering greater stakeholder trust while reducing operational costs.

AI complements blockchain by offering advanced capabilities in fraud detection, risk assessment, predictive analytics, and regulatory compliance [15]. AI can analyse vast amounts of transactional data in real time through machine learning algorithms and data-driven insights, identifying suspicious activities and mitigating risks before they escalate. AI-powered solutions also enhance Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures by detecting fraud patterns, improving regulatory compliance, and ensuring adherence

to legal frameworks [16]. Additionally, AI-driven automation streamlines financial processes, minimizing operational inefficiencies and reducing human errors.

The convergence of blockchain and AI creates a powerful synergy in addressing the challenges of digital finance [17]. While blockchain ensures trust through decentralization and immutability, AI enhances analytical capabilities, predictive insights, and automated decision-making [18]. These technologies can transform the FinTech industry by establishing a secure, transparent, and efficient financial ecosystem. Numerous studies have highlighted significant technological advancements, particularly in computer science (see Table 1).

**Table 1**. **Research on computer science.**

| No | Title | Ref. |
|---|---|---|
| **1** | XBRL open information model for risk-based tax audit using machine learning. | [19] |
| **2** | Enhanced wearable strap for feminine using IoT. | [20] |
| **3** | Face emotion recognition based on machine learning: A review. | [21] |
| **4** | Healthcare diseases classification based on machine learning algorithms: A review. | [22] |
| **5** | Detection of SQL injection attacks based on supervised machine learning algorithms: A review. | [23] |
| **6** | Phishing website detection using several machine learning algorithms: A review paper. | [24] |
| **7** | Potential security issues in implementing IaaS and PaaS cloud service models. | [25] |
| **8** | Exploring the nexus of user interface (UI) and user experience (UX) in the context of emerging trends and customer experience, human-computer interaction, applications of artificial intelligence. | [26] |
| **9** | Distributed systems for artificial intelligence in cloud computing: A review of AI-powered applications and services. | [27] |
| **10** | Aspect-based sentiment analysis on Amazon product reviews. | [28] |
| **11** | Crowd detection using YOLOv3-tiny method and Viola-Jones algorithm at mall. | [29] |
| **12** | Utilization of internet of things on food supply chains in food industry. | [30] |
| **13** | Computational thinking: The essential skill for being successful in knowledge science research. | [31] |
| **14** | Future trends in pharmaceuticals: Investigation of the role of AI in drug discovery, 3D printing of medications, and nanomedicine. | [32] |

This paper explores how blockchain and AI enhance trust in digital finance by securing transactions, preventing fraud, and ensuring regulatory compliance. Through a comprehensive analysis of real-world applications and potential future developments, the study examines how financial institutions, policymakers, and FinTech innovators can leverage these technologies to build a more resilient, secure, and transparent digital financial ecosystem. It also addresses the challenges of integrating blockchain and AI into FinTech solutions, including scalability issues, regulatory hurdles, and ethical considerations. The study employs a qualitative approach, incorporating a systematic literature review to achieve these objectives.

The novelty of this research lies in three key areas. First, it provides a comprehensive analysis of the combined impact of blockchain and AI on financial trust, a topic that has largely been studied in isolation. Second, it introduces a comparative framework for evaluating blockchain- and AI-based security mechanisms, offering a structured approach to assessing their effectiveness. Third, it identifies the practical challenges and regulatory considerations that must be addressed for large-scale adoption, providing valuable insights for both policymakers and financial institutions.

## 2. Research Method

This study employs a qualitative research approach, integrating a systematic literature review. A structured framework ensures thorough data collection, rigorous analysis, and reliable synthesis of findings. The methodology consists of the following steps:

i) Literature Selection: A comprehensive review was conducted on peer-reviewed academic journals, industry reports, white papers, and regulatory documents related to blockchain, AI, and digital finance. Selection criteria included relevance, credibility, and publication within the past five years.

ii) Data Collection: Relevant information was gathered from reputable databases such as IEEE Xplore, ScienceDirect, and Google Scholar.

iii) Data Analysis: A thematic analysis was performed to identify recurring patterns in adopting blockchain and AI within FinTech. Key areas of focus included security enhancement, fraud detection, identity verification, and compliance automation.

iv) Validation and Synthesis: Findings from the literature review and case studies were cross-referenced to ensure consistency and reliability. Emerging trends, challenges, and potential future developments were synthesized into a cohesive discussion.

A separate section provides detailed information on search strategies, data collection techniques, and analytical methods, thoroughly explaining how relevant literature was identified, evaluated, and synthesized [33-35].

## 3. Results and Discussion

### 3.1. Research trend

Figure 1 shows research trends on blockchain and AI in digital finance over the years, highlighting the increasing academic interest and publication volume in this field. This upward trajectory reflects the growing recognition of these technologies in enhancing security, transparency, and trust in FinTech solutions. A detailed explanation of the data acquisition process is provided in [36-39].

Figure 1 shows the research publication trends in blockchain, AI, and FinTech security. From 1989 to 2015, publication numbers remained relatively low, suggesting limited academic and industry interest in these technologies. This trend may indicate that blockchain and AI are still in their early stages or have yet to gain significant traction in the financial sector. However, after 2016, research activity increased significantly, reflecting a growing focus on these technologies-likely

driven by advancements in blockchain, the expanding use of AI in finance, and heightened concerns over cybersecurity and digital trust.

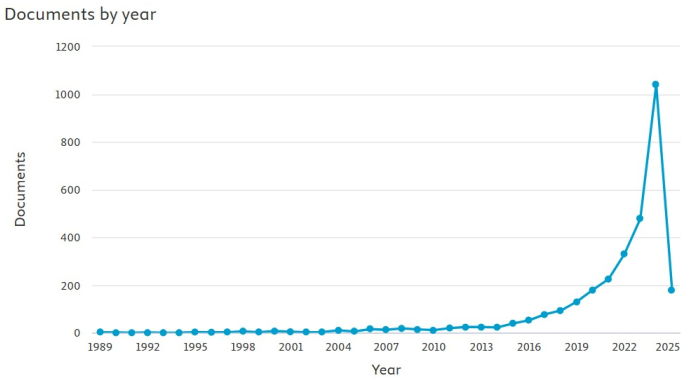


**Fig. 1. Number of publications related to blockchain, AI, and FinTech security based on the Scopus database.**

A sharp surge occurred after 2020, with publication volume rising exponentially and peaking in 2024 at over 1,000 studies. This trend suggests a strong interest in integrating blockchain and AI into digital finance, fuelled by rapid technological developments and the demand for secure, transparent financial systems. However, in 2025, the graph shows a steep decline, which may be due to incomplete data for the current year, shifting research priorities, or a potential saturation of studies on the topic.

## 3.2. Research contributions by country in blockchain and AI for digital finance

The global digital finance research landscape on blockchain and AI reflects varying contribution levels across different countries. Figure 2 shows the distribution of research publications by country, highlighting the nations that have made significant advancements in this field. This comparison offers valuable insights into the geographical concentration of research efforts and the influence of different economies in shaping the future of FinTech innovations.

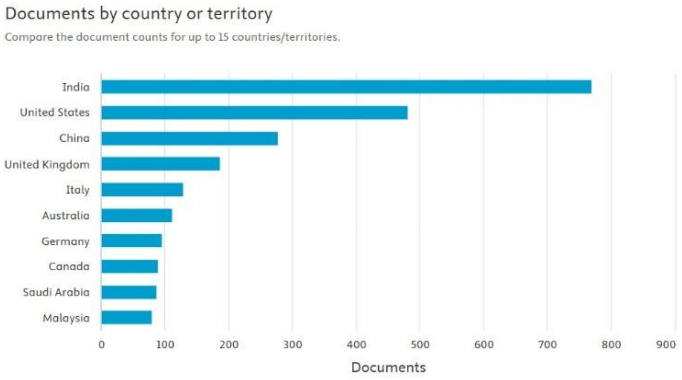


**Fig. 2. Research contributions by country in blockchain and AI for digital finance.**

Figure 2 shows a comparative analysis of research contributions from various countries in blockchain and AI for digital finance. India is the leading contributor, producing the highest number of research publications, followed by the United States and China. This trend underscores these nations' strong commitment to advancing financial technology, driven by rapid digital transformation, government initiatives, and the growing adoption of blockchain and AI in the industry.

Several other countries, including the United Kingdom, Italy, Australia, Germany, Canada, Saudi Arabia, and Malaysia, also demonstrate significant research activity in this field. The widespread global engagement highlights the increasing recognition of blockchain and AI as essential technologies for enhancing security, transparency, and efficiency in FinTech solutions. The data suggests that countries with well-established financial and technological infrastructures are leading research efforts to optimize digital financial ecosystems.

### 3.3. Distribution of research documents by type

The classification of research documents by type provides valuable insights into the predominant formats used in scholarly publications on blockchain and AI for digital finance. Figure 3 shows the distribution of these publication types, emphasizing their significance within the field.

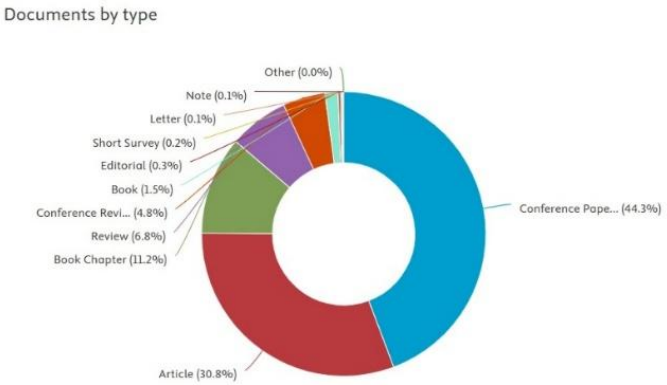


**Fig. 3. Distribution of research documents by type in blockchain and AI for digital finance.**

As shown in Fig. 3, conference papers constitute the largest share (44.3%), indicating that a substantial portion of research in this domain is presented at academic conferences, where emerging technologies and findings are actively discussed. Journal articles account for 30.8%, underscoring the crucial role of peer-reviewed publications in advancing knowledge.

Other notable categories include book chapters (11.2%), reviews (6.8%), and conference reviews (4.8%), reflecting a strong emphasis on synthesizing existing research and providing comprehensive overviews of technological developments. Less frequent contributions, such as books, editorials, short surveys, and notes, continue to shape academic discourse. This distribution underscores the dynamic nature of research dissemination in digital finance, with conferences and journal articles serving as the primary platforms for knowledge exchange and innovation.

### 3.4. Distribution of research documents by subject area

The distribution of research across subject areas underscores the interdisciplinary nature of studies on Blockchain and AI in digital finance. As shown in Fig. 4, various academic fields actively contribute to this rapidly evolving domain.

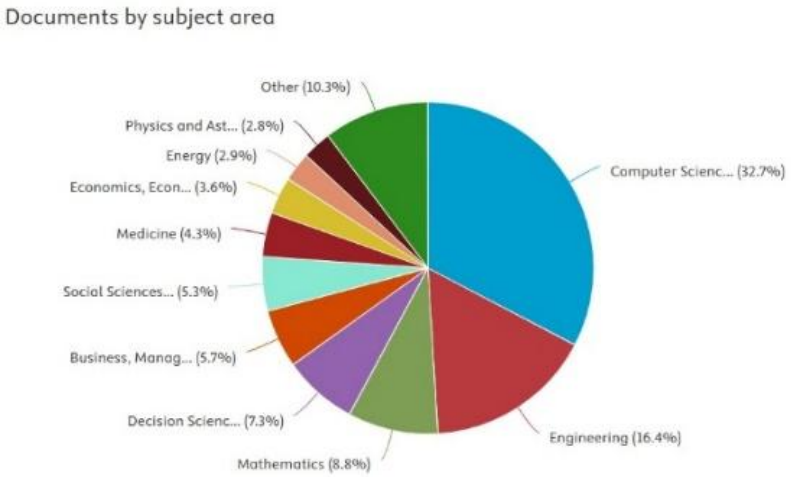


**Fig. 4. Distribution of research documents by subject area in blockchain and AI for digital finance.**

The distribution of research across subject areas highlights the interdisciplinary nature of studies on blockchain and AI in digital finance. Figure 4 shows the diverse academic fields contributing to this rapidly evolving domain. As shown in Fig. 4, Computer Science leads with 32.7%, underscoring its fundamental role in developing secure and transparent financial technologies. Engineering follows at 16.4%, emphasizing these innovations' technical and infrastructural aspects. Mathematics accounts for 8.8%, reflecting the importance of algorithms and cryptographic principles in financial security. Meanwhile, Decision Science (7.3%) and Business Management (5.7%) highlight a strong focus on financial decision-making, risk assessment, and strategic implementation.

Other notable contributors include Social Sciences (5.3%), Medicine (4.3%), Economics (3.6%), Energy (2.9%), and Physics & Astronomy (2.8%), showcasing the broad interdisciplinary interest in blockchain and AI applications. Additionally, the 10.3% categorized as "Other" suggests broader contributions that do not neatly fit into specific fields. This distribution highlights the multifaceted nature of blockchain and AI research, integrating computational, financial, and managerial perspectives to enhance trust and security in digital finance.

### 3.5. Blockchain for secure financial transactions

Blockchain technology has transformed financial transactions by providing a secure, decentralized, and transparent system for recording and verifying transactions [40]. Unlike traditional financial systems that depend on centralized entities such as banks and payment processors, blockchain operates on a distributed ledger where independent nodes validate each transaction. This decentralized

structure eliminates single points of failure and significantly reduces fraud risks, ensuring that financial records remain tamper-proof [41]. By utilizing cryptographic techniques such as digital signatures and hash functions, blockchain enhances security by preventing unauthorized modifications to financial data. Additionally, its transparency—where transaction records are publicly verifiable-fosters greater trust among consumers, businesses, and financial institutions [42].

One of blockchain's most notable advantages in financial transactions is its ability to support smart contracts, which automate agreements and execute transactions without intermediaries. This feature lowers costs, minimizes human error, and enhances efficiency in processes such as loan approvals, insurance settlements, and payments. Blockchain also streamlines cross-border transactions by eliminating the need for third-party verification, reducing both costs and processing times [43]. Another crucial application is identity management, enabling users to verify their identities without exposing sensitive information to centralized databases, thereby mitigating the risk of identity theft [44]. As financial institutions continue exploring blockchain's applications, its potential to enhance security, regulatory compliance, and fraud prevention is the key in shaping the future of digital finance.

Blockchain provides an immutable and decentralized ledger that enhances both transparency and security in financial transactions [40, 45, 46]. Its key benefits include:

i) Decentralization: Traditional financial systems rely on centralized authorities like banks to verify and process transactions. In contrast, blockchain operates on a decentralized network where multiple participants (nodes) validate transactions. This structure eliminates intermediaries, reducing fraud, corruption, and human error. Additionally, decentralization lowers transaction costs by removing third-party processing fees.

ii) Transparency: Every transaction recorded on a blockchain is publicly accessible and cannot be altered or deleted. This high level of transparency fosters trust among financial participants, as transaction histories remain verifiable and auditable. It is particularly valuable for financial institutions that must demonstrate regulatory compliance in digital finance.

iii) Security: Blockchain employs advanced cryptographic techniques like hash functions and digital signatures to secure financial data. Each transaction is stored in a block and linked to the previous block using a cryptographic hash, making it nearly impossible to alter data without network consensus. This structure protects against cyber threats, hacking attempts, and fraud.

iv) Smart Contracts: In FinTech applications, smart contracts automate processes such as loan approvals, insurance claims, and payment settlements. These self-executing agreements contain predefined rules written in code, automatically triggering transactions when conditions are met. By eliminating intermediaries, smart contracts reduce operational costs and minimize the risk of manipulation.

v) Cross-Border Transactions: Traditional international payments are slow, costly, and reliant on intermediaries. Blockchain streamlines cross-border transactions by enabling real-time, low-cost payments without third-party verification. Companies like Ripple and Stellar have developed blockchain-

based solutions to enhance the efficiency of global remittances and international financial systems.

vi) Identity Management: Financial institutions can leverage blockchain to verify client identities without storing sensitive data in centralized databases, reducing the risk of identity theft and data breaches. Blockchain-based identity management solutions empower individuals to control their digital identities securely.

vii) Resilience and Fraud Prevention: Unlike traditional databases, which are vulnerable to hacking, blockchain operates on a distributed ledger where data is replicated across multiple nodes. The data remains secure even if one node is compromised, ensuring resilience against cyberattacks. This security significantly reduces fraudulent transactions and strengthens trust in digital financial ecosystems.

Blockchain has already demonstrated its potential in securing digital finance through applications in cryptocurrency transactions, smart contracts, and cross-border payments. As adoption continues to grow, its role in enhancing security, efficiency, and transparency in financial systems is expected to expand further.

### 3.6. AI for fraud detection and risk assessment

AI is revolutionizing fraud detection and risk assessment by analysing vast real-time datasets to identify suspicious activities with greater accuracy. Unlike traditional methods, AI continuously learns from past fraud patterns and adapts to emerging threats, enhancing its ability to detect anomalies [47]. Beyond fraud detection, AI strengthens risk assessment by integrating diverse data sources for credit scoring, allowing financial institutions to make more informed lending decisions [48]. Additionally, AI streamlines regulatory compliance by automating processes, detecting money laundering patterns, and personalizing security measures based on user behaviour. By leveraging AI-driven solutions, financial services become more secure, efficient, and reliable, fostering a more resilient digital financial ecosystem [49-51].

i) Fraud Detection and Prevention: AI-powered fraud detection systems use machine learning algorithms to analyse vast transaction datasets and identify anomalies in real time. Continuously learning from historical fraud patterns, these systems adapt to emerging threats. By detecting unusual behaviours - such as unauthorized access, rapid transactions, or location inconsistencies - AI enables financial institutions to prevent fraud before it occurs.

ii) Risk Assessment and Credit Scoring: AI enhances credit risk assessment by incorporating alternative data sources, such as transaction history, online behaviour, and social media activity. Unlike traditional models that rely solely on financial records, AI-driven systems create a more comprehensive risk profile. This approach allows financial institutions to make informed lending decisions while expanding credit access to individuals without conventional credit histories, promoting financial inclusion.

iii) Automated Regulatory Compliance and Anti-Money Laundering (AML) Detection: Staying compliant with evolving regulations is a significant challenge in digital finance. AI automates transaction monitoring, detects suspicious activities, and identifies money laundering patterns in real time.

By flagging unusual transactions and generating automated reports, AI-powered compliance systems reduce manual effort while improving accuracy and efficiency.

iv) Behavioural Analytics for Fraud Prevention: AI analyses behavioural biometrics—such as typing speed, device usage, and mouse movements - to detect anomalies in user behaviour. If suspicious activity occurs, such as an unusual login location or erratic transaction patterns, AI triggers additional security measures, like multi-factor authentication, to mitigate risks.

v) Predictive Analytics for Market Risk Management: AI-driven predictive models assess market risks by analysing financial trends, economic indicators, and geopolitical events. Financial institutions leverage these insights to anticipate potential risks and adjust investment strategies. Hedge funds and investors also use predictive analytics for data-driven decision-making, helping them minimize losses during market volatility.

vi) Personalized Security Solutions: AI enhances fraud prevention by tailoring security measures to individual user behaviour. By continuously learning from a user's transaction history and interaction patterns, AI establishes personalized security thresholds, balancing robust protection with a seamless user experience.

Table 2 shows the respective functions and effectiveness levels of AI-based fraud detection techniques to provide a more precise comparison. Table 2 compares various AI-driven fraud detection methods based on their functionality and effectiveness in identifying fraudulent activities in financial transactions. Among these, machine learning and neural networks are the most effective. Machine learning excels at detecting transaction patterns, while neural networks identify complex fraud anomalies. Natural Language Processing (NLP) has moderate effectiveness in analysing textual data for suspicious activities, whereas predictive analytics forecasts potential fraud risks based on historical data. Rule-based systems flag anomalies using predefined rules that are the least adaptive and have low to moderate effectiveness.

**Table 2. Comparison of AI-driven fraud detection methods.**

| AI Technique | Function | Effectiveness |
|---|---|---|
| **Machine Learning** | Identifies fraudulent patterns in transactions | High |
| **Neural Networks** | Detects complex fraud patterns and anomalies | Very high |
| **Natural Language Processing (NLP)** | Analyses textual data for suspicious activities | Moderate |
| **Rule-Based Systems** | Uses predefined rules to flag anomalies | Low to moderate |
| **Predictive Analytics** | Forecasts potential risks based on past data | High |

The Table also highlights that advanced AI techniques, such as neural networks and machine learning, achieve the highest fraud detection accuracy by continuously learning and adapting to emerging threats. In contrast, though functional, rule-

based systems lack flexibility against evolving fraud tactics. Financial institutions can strengthen fraud detection by integrating multiple AI techniques - leveraging machine learning for adaptability, neural networks for complex pattern recognition, and predictive analytics for proactive risk assessment. This hybrid approach enhances fraud prevention, creating a more resilient digital finance ecosystem.

### 3.7. The synergy of blockchain and AI in digital finance

Table 3 shows how blockchain and AI complement each other in key areas of digital finance. By combining blockchain's security and transparency with AI's intelligence and adaptability, these technologies enhance efficiency, security, and trust in financial ecosystems. The Table highlights their synergistic benefits, enabling financial institutions to strengthen security, streamline operations, and ensure regulatory compliance. Blockchain's decentralized and immutable structure, paired with AI's advanced data processing and predictive analytics, creates a powerful framework for innovation in digital finance.

**Table 3. Synergy between blockchain and AI in digital finance.**

| Aspect | Role of Blockchain | Role of AI | Blockchain and AI Synergy |
|---|---|---|---|
| **Smart Contracts** | Provides automated contracts with predefined rules | Analyses real-time data for adaptive decision-making | More flexible and secure smart contracts |
| **Identity Verification** | Decentralized and encrypted digital identity system | Detects anomalies in login patterns or transactions | Enhanced security for digital identities |
| **Predictive Analytics** | Provides secure and immutable data storage | Identifies market trends and potential threats | More accurate data-driven decision-making |
| **Regulatory Compliance** | Ensures transparent and permanent audit trails | Automates transaction monitoring to detect anomalies | Faster and more efficient compliance processes |
| **Data Processing** | Ensures financial data integrity through decentralization | Processes large datasets at high speed | More efficient financial operations |
| **Cybersecurity and Threat Detection** | Prevents hacking with a decentralized structure | Identifies and mitigates cyber threats proactively | Smarter and more responsive security systems |

The integration of blockchain and AI unlocks groundbreaking opportunities to enhance security, efficiency, and trust in digital finance [52]. Their synergy enables:

i) Automated Smart Contracts – AI enhances blockchain-based smart contracts by enabling adaptive decision-making based on real-time data. Unlike traditional

contracts that follow static rules, AI-driven contracts incorporate fraud detection, risk assessment, and predictive analytics, making financial agreements more secure, flexible, and intelligent.

ii) Enhanced Identity Verification – AI-powered authentication detects suspicious login attempts, unusual transactions, and fraudulent activity, while blockchain ensures digital identity integrity through a tamper-proof ledger.

iii) Predictive Analytics for Financial Security – AI leverages blockchain's secure and immutable data to analyse market trends, assess risks, and detect fraud. This proactive approach helps financial institutions optimize risk management and investment strategies.

iv) Regulatory Compliance Automation – AI-driven monitoring identifies real-time anomalies, ensuring regulatory adherence, while blockchain's transparent ledger provides an immutable audit trail for enhanced accountability.

v) Efficient and Secure Data Processing – Blockchain preserves data integrity, while AI rapidly analyses large financial datasets, reducing operational costs, enhancing decision-making, and improving customer experience.

vi) Cybersecurity and Threat Detection – Blockchain's decentralized structure strengthens security against breaches, while AI monitors and mitigates cyber threats, ensuring proactive fraud prevention

The fusion of blockchain and AI is shaping the future of digital finance, fostering an ecosystem where transactions are more secure, compliance is automated, and fraud prevention is more sophisticated. As these technologies evolve, their combined potential could further redefine trust and innovation in FinTech.

## 4. Conclusion

The integration of blockchain and AI is revolutionizing security, transparency, and trust in digital finance. Blockchain's decentralized framework ensures tamper-proof transactions, while AI-driven analytics enhance fraud detection, risk assessment, and regulatory compliance. These technologies address financial fraud, identity verification, and market stability, fostering a more resilient and efficient financial ecosystem. However, challenges remain. Regulatory complexities, interoperability issues, and high implementation costs hinder widespread adoption. Overcoming these barriers requires ongoing research, cross-industry collaboration, and continuous innovation. By refining these technologies, the financial sector can unlock its full potential-creating a more secure, inclusive, and resilient digital financial environment that benefits consumers and institutions.

## References

1. Jadhav, S.D.; and Shawale, V.D. (2022). A study of awareness and preference of urban investors toward digital gold as an investment option and its correlation to the level of education. *ASEAN Journal of Economic and Economic Education*, 1(2), 79-88.
2. Damayanti, F.N.; Kusmawati, P.; Navia, V.; and Luckyardi, S. (2022). Readiness the owner of small medium enterprises for digital financial records

in society 5.0 era. *ASEAN Journal of Economic and Economic Education*, 1(1), 1-8.

3. Josyula, H.P.; and Expert, F.P.T. (2021). The role of fintech in shaping the future of banking services. *The International Journal of Interdisciplinary Organizational Studies*, 16(1), 187-201.
4. Kiran, D.; and Verma, V. (2024). The role of financial technology in reshaping global financial services and markets: Opportunities and risks. *Library of Progress-Library Science, Information Technology and Computer*, 44(3), 21753-21762.
5. Udeh, E.O.; Amajuoyi, P.; Adeusi, K.B.; and Scott, A.O. (2024). The role of big data in detecting and preventing financial fraud in digital transactions. *World Journal of Advanced Research and Reviews*, 22(2), 1746-1760.
6. Esmail, R.P.; Falsario, M.N.J.S.; Halaghay, B.E.R.; Luna, M.M.; Padua, J.N.J.D.; and Pasanso, R.G.D. (2022). Online selling: Unfolding the lifestyle of the working students. *ASEAN Journal of Economic and Economic Education*, 1(2), 89-94.
7. Khadka, M. (2022). A systematic appraisal of multi-factor authentication mechanisms for cloud-based e-commerce platforms and their effect on data protection. *Journal of Emerging Cloud Technologies and Cross-Platform Integration Paradigms*, 6(12), 12-21.
8. Sharf, A.; Akhtar, S.; Sharf, S.; and Asif, M. (2021). Ethical issues of cyberstalking and personal privacy in Pakistan: A literature survey. *Indonesian Journal of Multidisciplinary Research*, 1(2), 357-362.
9. Zachariadis, M.; Hileman, G.; and Scott, S.V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization*, 29(2), 105-117.
10. Zetzsche, D.A.; Arner, D.W.; and Buckley, R.P. (2020). Decentralized finance. *Journal of Financial Regulation*, 6(2), 172-203.
11. Pazarbasioglu, C.; Mora, A.G.; Uttamchandani, M.; Natarajan, H.; Feyen, E.; and Saal, M. (2020). Digital financial services. *World Bank*, 54(1), 1-54.
12. Al-Khassawneh, Y.A. (2023). A review of artificial intelligence in security and privacy: Research advances, applications, opportunities, and challenges. *Indonesian Journal of Science and Technology*, 8(1), 79-96.
13. Lizama, M.G.; Huesa, J.; and Claudio, B.M. (2024). Use of blockchain technology for the exchange and secure transmission of medical images in the cloud: Systematic review with bibliometric analysis. *ASEAN Journal of Science and Engineering*, 4(1), 71-92.
14. Manda, J.K. (2018). Implementing blockchain technology to enhance transparency and security in telecom billing processes and fraud prevention mechanisms, reflecting your blockchain and telecom industry insights. *Advances in Computer Sciences*, 1(1), 1-21.
15. Farayola, O.A. (2024). Revolutionizing banking security: Integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. *Finance and Accounting Research Journal*, 6(4), 501-514.
16. Otubu, R.O. (2024). Harnessing artificial intelligence to combat money laundering in cryptocurrency transactions. *Journal of Emerging Trends in Engineering and Applied Sciences* (*JETEAS*), 15(5), 168-176.

17. Bhumichai, D.; Smiliotopoulos, C.; Benton, R.; Kambourakis, G.; and Damopoulos, D. (2024). The convergence of artificial intelligence and blockchain: The state of play and the road ahead. *Information*, 15(5), 1-32.
18. Chowdhury, R.H. (2024). The evolution of business operations: Unleashing the potential of artificial intelligence, machine learning, and blockchain. *World Journal of Advanced Research and Reviews*, 22(3), 2135-2147.
19. Wibowo, B.D.S. (2022). XBRL open information model for risk based tax audit using machine learning. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 3(1), 21-46.
20. Kumar, S.; Nandhini, S.; and Sujitha, R. (2022). Enhanced wearable strap for feminine using IoT. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 3(1), 83-94.
21. Abdulazeez, A.M.; and Ageed, Z.S. (2024). Face emotion recognition based on machine learning: A review. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 5(1), 53-87.
22. Mohammed, A.; and Abdulazeez, A.M. (2024). Healthcare diseases classification based on machine learning algorithms: A review. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 5(2), 218-252.
23. Abdullah, H.S.; and Abdulazeez, A.M. (2024). Detection of SQL injection attacks based on supervised machine learning algorithms: A review. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 5(2), 152-165.
24. Veach, A.; and Abualkibash, M. (2022). Phishing website detection using several machine learning algorithms: A review paper. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 3(2), 219-230.
25. Erlangga, W.K.; and Ramadhan, M.R. (2022). Potential security issues in implementing IaaS and PaaS cloud service models. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 3(2), 143-162.
26. Paneru, B.; Paneru, B.; Poudyal, R.; and BikramShah, K. (2024). Exploring the nexus of user interface (UI) and user experience (UX) in the context of emerging trends and customer experience, human computer interaction, applications of artificial intelligence. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 5(1), 102-113.
27. Zangana, H.M.; and Zeebaree, S.R.M. (2024). Distributed systems for artificial intelligence in cloud computing: A review of AI-powered applications and services. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 5(1), 11-30.
28. Abubakar, M.; Shahzad, A.; and Abbasi, H. (2021). Aspect-based sentiment analysis on Amazon product reviews. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 2(2), 206-211.
29. Ginting, S.L.B.; Maulana, H.; Priatna, R.A.; Fauzzan, D.D.; and Setiawan, D. (2021). Crowd detection using YOLOv3-tiny method and Viola-Jones algorithm at mall. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 2(2), 125-134.

30. Maulana, H.; Ginting, S.L.B.; Aryan, P.; Fadillah, M.R.; and Kamal, R.N. (2021). Utilization of internet of things on food supply chains in food industry. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 2(1), 103-112.
31. Bachtiar, A.M. (2023). Computational thinking: The essential skill for being successful in knowledge science research. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 4(1), 11-22.
32. Paneru, B.; and Paneru, B. (2023). Future trends in pharmaceuticals: Investigation of the role of AI in drug discovery, 3D printing of medications, and nanomedicine. *International Journal of Informatics, Information System and Computer Engineering* (*INJIISCOM*), 4(2), 120-134.
33. Rochman, S.; Rustaman, N.; Ramalis, T.R.; Amri, K.; Zukmadini, A.Y.; Ismail, I.; and Putra, A.H. (2024). How bibliometric analysis using VOSviewer based on artificial intelligence data (using ResearchRabbit data): Explore research trends in hydrology content. *ASEAN Journal of Science and Engineering*, 4(2), 251-294.
34. Al Husaeni, D.F.; and Nandiyanto, A.B.D. (2022). Bibliometric using VOSviewer with publish or perish (using Google Scholar data): From step-by-step processing for users to the practical examples in the analysis of digital learning articles in pre and post covid-19 pandemic. *ASEAN Journal of Science and Engineering*, 2(1), 19-46.
35. Al Husaeni, D.N.; and Al Husaeni, D.F. (2022). How to calculate bibliometric using VOSviewer with Publish or Perish (using Scopus data): Science education keywords. *Indonesian Journal of Educational Research and Technology*, 2(3), 247-274.
36. Al-Khassawneh, Y.A. (2023). A review of artificial intelligence in security and privacy: Research advances, applications, opportunities, and challenges. *Indonesian Journal of Science and Technology*, 8(1), 79-96.
37. Azizah, N.N.; Maryanti, R.; and Nandiyanto, A.B.D. (2021). How to search and manage references with a specific referencing style using Google Scholar: From step-by-step processing for users to the practical examples in the referencing education. *Indonesian Journal of Multidiciplinary Research*, 1(2), 267-294.
38. Rahayu, N.I.; and Ismail, A. (2023). Trends in the use of artificial intelligence (AI) technology in increasing physical activity. *Indonesian Journal of Educational Research and Technology*, 3(3), 295-304.
39. Solihat, A.N.; Dahlan, D.; Kusnendi, K.; Susetyo, B.; and Al-Obaidi, A.S.M. (2024). Artificial intelligence (AI)-based learning media: Definition, bibliometric, classification, and issues for enhancing creative thinking in education. *ASEAN Journal of Science and Engineering*, 4(3), 349-382.
40. Abdulhakeem, S.A.; and Hu, Q. (2021). Powered by blockchain technology, DeFi (Decentralized finance) strives to increase financial inclusion of the unbanked by reshaping the world financial system. *Modern Economy*, 12(01), 1-16.

41. Mustyala, A. (2023). Leveraging blockchain for fraud risk reduction in fintech: Infrastructure setup and migration strategies. *EPH-International Journal of Science and Engineering*, 9(2), 1-10.
42. Rijal, S.; and Saranani, F. (2023). The role of blockchain technology in increasing economic transparency and public trust. *Technology and Society Perspectives* (*TACIT*), 1(2), 56-67.
43. Eyo-Udo, N.L.; Agho, M.O.; Onukwulu, E.C.; Sule, A.K.; Azubuike, C.; Nigeria, L.; and Nigeria, P. (2024). Advances in blockchain solutions for secure and efficient cross-border payment systems. *International Journal of Research and Innovation in Applied Science*, 9(12), 536-563.
44. Sung, C.S.; and Park, J.Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. *Journal of Enterprise Information Management*, 34(5), 1481-1505.
45. ElHassouni, L.; and Ouchekkir, A. (2024). Revolutionizing financial markets: The role of distributed ledger technology in payments, clearing, and settlements. *International Journal of Accounting, Finance, Auditing, Management and Economics*, 5(10), 198-226.
46. Owolabi, O.S.; Hinneh, E.; Uche, P.C.; Adeniken, N.T.; Ohaegbulem, J.A.; Attakorah, S.; and Nwariaku, H. (2024). Blockchain-based system for secure and efficient cross-border remittances: A potential alternative to SWIFT. *Journal of Software Engineering and Applications*, 17(8), 664-712.
47. Bello, O.A.; and Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer Science and IT Research Journal*, 5(6), 1505-1520.
48. Faheem, M.A. (2021). AI-driven risk assessment models: Revolutionizing credit scoring and default prediction. *Iconic Research and Engineering Journals*, 5(3), 177-186.
49. Turksen, U.; Benson, V.; and Adamyk, B. (2024). Legal implications of automated suspicious transaction monitoring: Enhancing integrity of AI. *Journal of Banking Regulation*, 25(4), 359-377.
50. Aziz, L.A.R.; and Andriansyah, Y. (2023). The role of artificial intelligence in modern banking: An exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, 6(1), 110-132.
51. Devan, M.; Prakash, S.; and Jangoan, S. (2023). Predictive maintenance in banking: Leveraging AI for real-time data analytics. *Journal of Knowledge Learning and Science Technology*, 2(2), 483-490.
52. Martinez, D.; Magdalena, L.; and Savitri, A.N. (2024). AI and blockchain integration: Enhancing security and transparency in financial transactions. *International Transactions on Artificial Intelligence*, 3(1), 11-20.