Journal of Techniques, ISSN: 2708-8383, Vol. 8, No. 2, 2026, Pages 48-57
https://doi.org/10.51173/jt.v8i2.2829

JOURNAL OF TECHNIQUES

Journal homepage: http://journal.mtu.edu.iq

REVIEW ARTICLE - ENGINEERING (MISCELLANEOUS)

A Systematic Literature Review of Computer-Based Blockchain Enhancements Using AI Techniques as an e-Governance Security

Mohammed Salem Atoum[1], Ghalib Ahmed Salman[2*], Zahraa Abbas Hamza[2], Zena Ahmed Alwan[2], Ahmed Husham AL-Badri[3]

[1]Computer Science Department, King Abdulla II School of Information Technology, The University of Jordan, Amman, Jordan

[2]Department of Artificial Intelligence, Technical College of Artificial Intelligence, Middle Technical University, Baghdad, Iraq

[3]Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia

[*] Corresponding author E-mail: dr.ghalib@mtu.edu.iq

Article Info.

Article history:

Received
25 December 2025

Revised
21 May 2026

Accepted
02 June 2026

Published
30 June 2026

Abstract

Blockchain applications have adopted various techniques over the past decade, and one revolutionary approach has been the use of Artificial Intelligence (AI). They had crucial roles in the transparency and security of e-Governance applications. In this paper, the interrelated impacts of AI techniques in enhancing Blockchain applications are illustrated to ensure transparent and secure e-Governance services against forgery and intrusion. By reviewing available articles, this paper discusses the role and capabilities of AI in influencing and manipulating large volumes of data related to Blockchains, which build stubborn, robust, and stable e-governance. The conclusions of this paper reveal that adopting AI techniques in Blockchain applications significantly enhances security and transparency by enabling simultaneous detection of system abnormalities. Concluded outcomes highlight major expectations for Blockchain AI Combination (BAIC) techniques to enhance e-government frameworks and financial transactions, emphasizing their potential to support global achievements by promoting greater transparency and security in economic environments. In this review, deeper and broader research into the scalability of Blockchain combined with AI techniques is proposed to address various aspects of e-governance.

Publisher: Middle Technical University

Keywords: Blockchain; Artificial Intelligence; Financial Transaction; e-Governance.

1. Introduction

The e-governance applications witnessed significant integrations by adopting state-of-the-art techniques such as Blockchain and different applications of Artificial Intelligence (AI) [1]. Such versions were leveraged for serious e-governance applications, such as intrusion detection, operational weaknesses, and financial transaction transparency at higher levels [2, 3]. As e-governance services continually expand, there is a crucial need for transaction methods that offer higher security and efficiency [2, 4]. Transparency and security of e-governance applications leveraging significant benefits from the Blockchain and AI Combination (BAIC), even when using each of them [5]. One of the most powerful aspects of AI applications is their ability to handle large amounts of data in real time. Such attributes make AI applications active and efficient at detecting forgery intrusions and estimating potential risks. On the other hand, Blockchain systems share common attributes, such as decentralization and immutability, to ensure transparency and integrity of information in e-governance operations [6].

E-governance services handled different aspects and applications, yet financial services were the most closely related to blockchain, especially since much of the literature connects Bitcoin and financial applications to Blockchain systems [7]. Discussing financial transparency has been a focus since the most relevant applications were the financial ones [4]. AI was also adopted across various financial applications, especially for future planning, fraud detection, and risk management [8, 9]. Such abilities enable states and financial centers to detect fraud and reduce errors [7]. This paper reviews articles on Blockchain related to financial security, transparency, and authentication. Notably, ordinary systems in financial services pose non-negligible challenges [8]. BAIC systems handled such challenges efficiently, and the next section discusses BAIC's building structure. Specifically, this review intends to discuss BAIC articles on financial transactions and their transparency, security, and efficiency, and to examine Blockchain applications across different aspects of e-governance.

Nomenclature and Symbols			
AI	Artificial Intelligence	ML	Machine Learning
BAIC	Blockchain and AI Combination	DL	Deep Learning
DLT	Distributed Ledger Technology	EMR	Electronic Medical Record
CDBC	Central Bank Digital Currencies		

2. BLOCKCHAIN and AI Combination (BAIC)

In this section, a brief preview is provided to discuss the fundamentals, structure, and general aspects of BAIC, focusing on how combining these technologies ensures secure, transparent, and robust financial services. Fig. 1 shows a theoretical taxonomy of how BAIC aspects are connected to AI applications. Furthermore, AI techniques integrated financial applications and blockchains into risk management [10]. The next sections discuss the general characteristics of AI and Blockchain, as well as their differences and similarities.

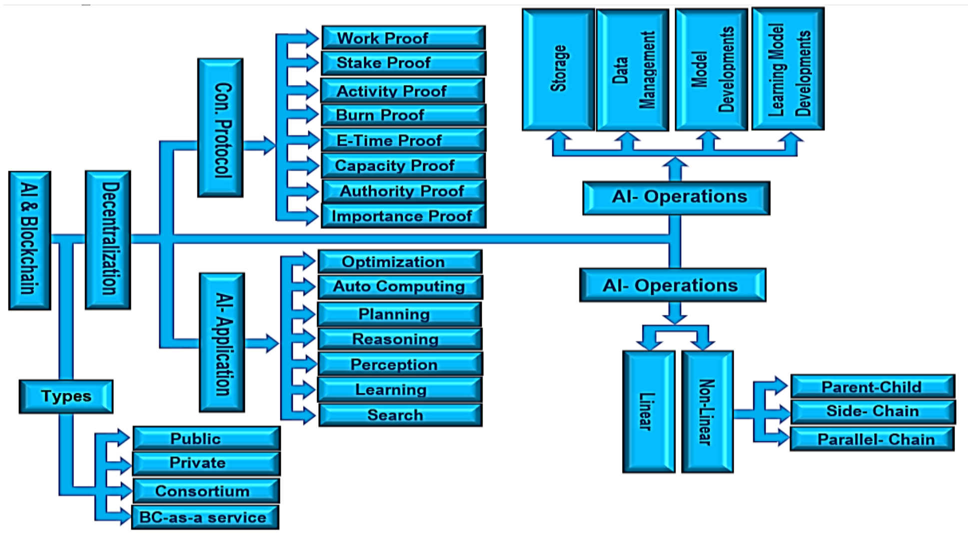

Fig. 1. The general taxonomy that connects AI techniques with Blockchain applications

2.1. Blockchain

The primary driver of Blockchain's evolution was the emergence of Bitcoin in the first decade of this century [11, 12]. From this, various Distributed Ledger Technologies (DLTs) emerged as cornerstones of applications in Cybersecurity, Finance, Business, and Healthcare [13, 14]. Different e-governance systems leverage blockchain applications to enhance e-governance services with greater transparency and confidence [6, 8, 15]. It was recently highlighted that most countries worldwide are adopting (or discussing adopting) Central Bank Digital Currencies (CBDCs) [16], indicating the expanding application of blockchain technologies. Such adoption offers transformative abilities for financial issues and other e-governance applications. Thus, different challenges like quick and smooth transactions, scalable applications, efficient energy use, and dynamic adaptability [17]. In most of the blockchain applications, adopted techniques ensure efficient transaction tracking and simultaneously update information over the whole Blockchain [18]. Using the decentralization concept, transactions are ensured to be trusted, with their initialization, modification, or deletion requiring consensus among all chain participants using efficient error-reduction techniques [19, 20]. Besides error reduction, strengthening the chain against intrusion attacks must also be ensured [21]. The term TRUST in blockchain concepts includes free, intermediate, and secure transactions [5, 14, 21]. To build a successful blockchain system, some characteristics are crucial to ensure for all distributed projects, such as:

- Decentralization: This aspect ensures the creation of a distributed system that does not rely on a central point of authority to control the whole system. This is to publicly spread user data across the chain to nodes [22]. Blockchain robustness against attacks is ensured using specific network configurations and security protocols [19].
- Anti-Censorship: In open blockchains, where no permissions are required for all participants, anti-censorship is crucial. All transactions are recorded in the Blockchain ledger using a consensus mechanism, which, by design, makes it difficult to control the ledger's contents. On the other hand, permissioned blockchains are constrained by a membership model, with varying levels of censorship resistance depending on who is a member at the time [23, 24]. Yet, such a type offers greater robustness against Blockchain censorship than a centralized ledger [25].
- Stability: It is an essential blockchain attribute that combines a decentralized architecture with consensus mechanisms. Typical decentralized consensus prevents intrusion modifications, whereas any modification to Blockchain data can be made only under the consensus of all participants connected to the network [26, 27].
- Secure ledger: In blockchain systems, security features are crucial, such as anti-counterfeiting and transaction tracing [28, 29]. Such attributes provide efficient tools for data safety and integrity, particularly in sensitive domains such as medical records [30, 31]. Adopting blockchain techniques, especially when combined with AI algorithms, provides significantly greater security for adopting organizations by protecting transactions against tampering and intrusions.
- Hidden Identity: Blockchain applications enable participants to access multiple addresses, enhancing network privacy and preventing third parties from accessing personal information. Although it provides a significant level of anonymity, optimal privacy is not guaranteed due to limitations of the Blockchain [32, 33].

- Transparency: Transaction details in Blockchain networks are mostly transparent to be viewed by network nodes [12, 34]. Due to the decentralization concept, blockchain networks support the entire network, including all active nodes [5]. Transparency ensures that all nodes can view transaction information. For node synchronization, announce their ledger and all of their transaction records over the network. In this way, each node remains aware of up-to-date transactions occurring within the blockchain [6].

2.2. Artificial intelligence (AI)

Artificial intelligence (AI) approaches were adopted not only to enhance Blockchains but also for tasks previously performed by humans, such as medical diagnosis [35], person identification [36], age and gender estimation [37], and farming and weed management [38]. In other words, the primary goal of AI algorithms is to enable machines to simulate human intelligence and make decisions previously made only by humans. AI can be briefly defined to accomplish the next goals [39]:

- Acting humanely and rationally
- Thinking humanly and rationally

AI can also be referred to as providing machines with the ability to think like humans, as currently elucidated by [7]. Therefore, AI techniques are recognized as distinct from traditional algorithms, as they can learn and adapt to data and results [40]. Such abilities enable AI techniques to accomplish higher-complexity tasks. Recent developments in AI approaches that produced interactive applications (such as Chat GPT, Gemini, and others) have recorded considerable abilities in collecting, analyzing, and handling huge amounts of information (data). Such applications are built on complex architectures that enable them to store their information in unconventional ways [41]. Some of the AI characteristics can be listed as follows [42]:

- Data ingestion: The most powerful AI techniques are learning algorithms (Machine Learning and Deep Learning) [38, 43], which enable AI to handle large volumes of data from different sources independently. Such attributes reduce (delete) errors made under human factors to minimize any inaccuracy in handling AI data [6]
- Machine Learning: Analyzing and learning from experiments is a major goal of AI-based systems, enabling them to handle future situations and simulate human intelligence [40, 44]. Two different approaches of learning were adopted in different AI applications, Machine Learning (ML) and Deep Learning (DL), where they have a common task of learning, yet ML algorithms depend on candidate representatives to learn from, while DL algorithms exclude the representation stage and build their learning on a huge amount of the whole object [45]. Different examples of learning results are observed in Autonomous Cars, Self-Driving cars, and smart games, among others [46].
- Free Style: Already-designed algorithms were widely adopted to provide a roadmap for the computer to follow, while new AI concepts adopt an independent style in handling and solving problems. Such independence and free style provide more adaptive and dynamic solutions due to the variety of problems [47].
- Reasoning: Far more advanced than ordinary computer algorithms, AI applications handle learned information rather than relying solely on data, enabling meaningful conclusions and informed decisions [48]. Efficient reasoning enables AI applications to solve processes designed by humans, which is pivotal for machine refinement [49].
- Symbol-Based Algorithms: Most AI algorithms extract information from symbols rather than raw data, where symbols are widely used to represent events and objects, which are first transformed into strings, then into symbols, before they are handled [50]. This explains the symbol's relationship, where most modern AI-based learning, detection, and classification problems handle images, waves, or signals [51].

2.3. Limitations and contradictions against the BAIC combination

Besides considerable enhancements achieved with the BAIC combination, significant limitations also limited its performance. It is worth noting that people share financial information, details, and transactions, thus it is reasonable to be cautious of potential loss. Some major limitations are indicated in sharing financial transactions over traditional Blockchains or even BAIC applications [3, 52], such as:

- data storage and security
- interoperability of BAIC-based financial transactions
- digital-transaction decentralizing
- transaction trust and data transparency

It is widely known that most owners of financial transactions DONOT prefer to disclose their financial details [27], so most of the collected information for the BAIC-model training [53] is inaccurate. To build a robust BAIC system that addresses such limitations, most applications tend to balance information sensitivity, transaction protection, and public [8]. To guarantee the best possible standards worldwide and the collection of data, optimal approaches must be defined [54]. Thus, a BAIC application can revolutionize financial transactions on the Blockchain network if provided with transparent, secure data [30]. Using privacy-preserving (encryption) approaches, AI techniques enhance Blockchain applications by improving transaction and data security, computational decentralization, and security against untrusted terminals [21]. Distributed ledgers in BAIC systems store and exchange encrypted data in an immutable, secure, and authenticated manner [30]. BAIC networks are block-based, connected networks that continuously preserve transactions, with each document timestamped and unaltered [18]. As a result, AI techniques enhance machines' ability to analyze, understand, and classify objects and events in their environment, enabling them to make informed decisions and simulate human behavior.

3. Methodology

In this review, the PRISMA protocol was utilized to build a Systematic Literature Review (SLR) using software tools to combine Blockchain Application with AI techniques (BAIC) to enhance financial operations in e-governance systems. PRISMA methodology [1] was proposed with extensive searches on Google Scholar, Springer, Elsevier, and IEEE, producing the consideration of (113) different articles that are relevant to the reviewed subject. Search keywords adopted in this work included “Financial operations in Blockchain,” “Blockchain and AI combination,” “Blockchain supported by AI Techniques,” “AI enhancements on financial transparency,” “Blockchain and AI integration,” “Blockchain and deep learning network,” “Deep Reinforcement Learning in Blockchain applications,” “Secure financial transaction in Blockchain,” “Financial transaction supply chain management," "Adopting AI and Blockchain to enhance Bank operations and supply chain," "AI techniques enhance overseas Banking," "Blockchain ignoring AI techniques,". This review combined Narrative Literature Review (NLR) with bibliometric approaches, with a main focus on comprehensive articles that advance understanding of the occurrence of financial transactions in Blockchain. Irrelevant articles without analytical discussion were excluded (hypothetical discussions, posters, and conference abstracts). The PRISMA methodology for reporting BAIC-related citations adopted in this review is illustrated in Fig. 2, which details the procedures used to select the 113 articles. The current strategy in the selection process can be overviewed in the following:

- Google Scholar, Springer, Elsevier, and IEEE databases were adopted to download relevant articles.
- Initial results of the download included 319 articles from Springer, 586 from ELSEVIER, 231 from IEEE, and 736,622 from Google Scholar, for a total of 736,758 articles.
- Each article was monitored for its Title and Abstract to apply exclusion criteria, resulting in the exclusion of 716247 records.
- EndNote software (Clarivate Analytics) was adopted to exclude duplicates, using the "Find Duplicates" option [55], which removed 10620 records.
- Article Qualification: the remaining 9891articles were considered to exclude non-relevant ones, which excludes 8376 articles, and the remaining 1515 articles were qualified to consider full text screening.
- Data Sufficiency consideration: insufficient-data articles (lack of topic relevance) were excluded, resulting in the exclusion of 1402 articles and the retention of 113 qualified articles that underwent further study to build this review.

Previously published articles on combining Blockchain applications with AI techniques have stated that such a combination is efficient and robust against various challenges, including security, privacy, and reliability. This paper reviews published articles on BAIC applications, providing a precise, efficient, and holistic investigation of the BAIC combination. Reviewed articles were published within the 2020- 2025 period. In-depth analysis was conducted in this review to provide a qualitative scientific approach for reviewing published articles and studies that discussed BAIC integration to achieve successful financial transactions. This study qualitatively investigates academic and industrial publications that examine the mutual effects of AI techniques and Blockchain applications. The major stated motivation for such a combination was to ensure stable, transparent, and secure financial operations. In contrast, this review aims to analyse these publications to holistically understand how BAIC enhancements are significant in this sector. This review enhances its methodology with analytical measures to deepen the holistic understanding; in addition, quantitative results on performance with/without the BAIC combination highlight the mutual enhancements between them. In the next sections, this review attempts to answer the following research questions:

- What are the enhancements provided by combining them?
- What are the conflicts between them?
- What are the performance levels and characteristics of them with/ without combination?
- After their convergence, how will these two technologies be applied to the real world?
- What are the challenges and future trends?

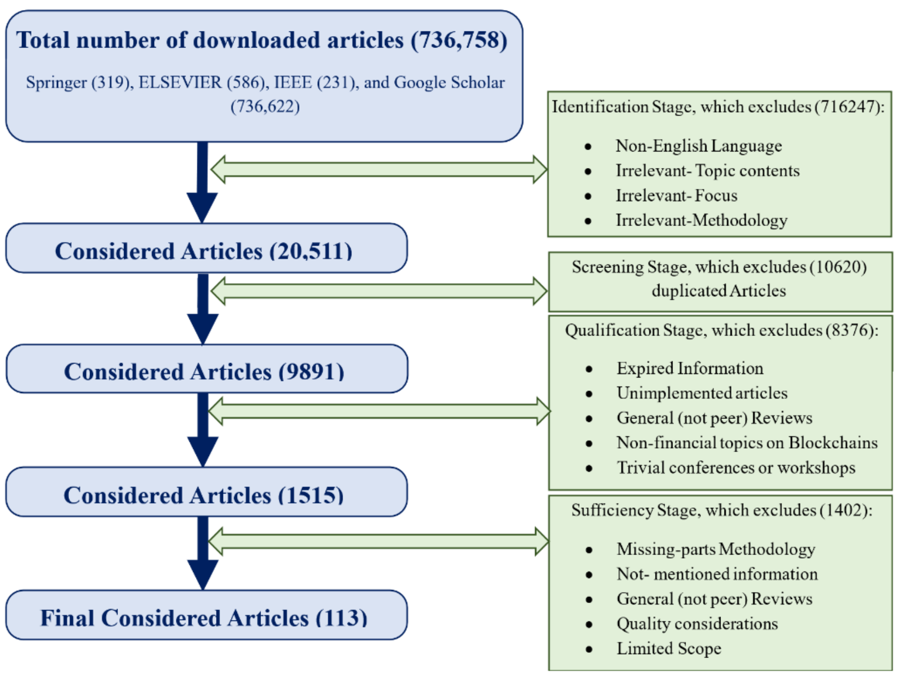

Fig. 2. Article exclusion and selection process depending on the PRISMA protocol

3.1. Resource collection

Data collection is an essential part of any BAIC system, where it is necessary for system transparency, stability, and security. To diversify, this study reviewed various article types, including scientific papers, problem-solving reports, and case-study papers, to ensure a broad understanding. All articles were verified to be from reputable sources to build this review on a solid foundation, enabling discussion of the most recent enhancements, innovations, and solutions. On the other hand, this review discussed procedural understanding, theoretical analysis of BIC developments, implementation challenges, and successful experiments conducted by various institutions in financial e-governance. A comprehensive view was built by combining analytical evidence with theoretical perspectives that explain significant BAIC enhancements in e-governance systems. Different sources were used to feed this review, such as:

- Scientific Articles: journal papers that discussed the financial aspects of e-governance and yielded enhancements that occurred depending on the BAIC combination.
- Case Studies: different financial states and centers produce periodical manipulations of real cases that examine and integrate financial transactions, where BAIC enhancements are significantly obvious.
- Industrial Experiments: evaluation reports constructed depending on successful industrial experiments on e-governance institutions, where such reports discuss PowerPoint, challenges, and weakness points of BAIC. Such reports indicate practical examples and real-world impacts of transparency, security, and stability of financial transactions.

The selection parameters were enhanced to ensure efficient and precise discussion of case studies, where they were selected due to:

- Combination level between AI and Blockchain.
- Different circumstances and areas of BAIC applying.
- The ability to access data after implementation.

Table 1 presents the publications downloaded over the review period (2019-2025), grouped by publication year and publication type: scientific articles, industrial reports, and case studies. Some of them were excluded because their subjects were too far away, while others were excluded because their methodologies or results were unclear.

Table 1. Roadmap of downloaded publications for this review

Publication Year	Scientific Articles	Industrial Reports	Case Studies	Total
2019	9	3	0	12
2020	12	0	1	13
2021	11	3	3	17
2022	14	2	0	16
2023	17	4	3	24
2024	20	2	3	25
2025	9	3	2	14
Total	84	17	12	113

3.2. Challenge determination

Various challenges to the BAIC application were identified to assess BAIC efficiency, as these challenges affect the financial sector of e-governance. Common challenges with BAIC usually arise from the complexity of AI and/or Blockchain techniques. Scalability, Stability, and complexity are major sources of these challenges in applying BAIC systems. Practical challenges like time consumption and the required cost for the BAIC application, which is also affected by other challenges related to data compliance and privacy. This is important to address due to the ongoing development of BAIC legal legislation [1, 12]. Getting a sufficient overview of these challenges provides precise assessments of the effects, benefits, and drawbacks of combining AI techniques with Blockchain systems. More details on the different challenges [56] BAIC faces are illustrated in Fig. 3.

3.3. Analytical framework

This review uses a comparative analysis as the general framework, employing to assess all relative enhancements in the transparency, security, and stability of data in BAIC financial-transaction systems.

3.4. Comparing case studies

Comparing different Case-Study publications indicates that e-governance systems worldwide have adopted a wide range of approaches to implement BAIC systems [57]. Therefore, it was also noted that specific patterns were repeatedly emphasized, such as financial fraud detection using AI algorithms. Investing in AI techniques in Blockchain systems has yielded notable improvements in stability, transparency, and security, with some blockchain systems and centers having considerable BAIC investments [21, 58]. Such that noticeable improvements were achieved, including enhanced auditability of financial transactions and greater confidence in detecting counterfeit blockchain records [59]. In addition, various researchers have noted that Blockchain systems and centers have faced notable obstacles due to regulations and high costs [60], and they suggested that achieving optimal success in secure blockchain transactions requires careful and thorough planning despite the benefits of this field [61]. The next section presents a scientific analysis of the research's advantages/ disadvantages in terms of transaction security and blockchain transparency, using the BAIC combination.

Fig. 3. Different challenges to implementing BAIC systems

4. Achievement Analysis

This section analyzes real-world case studies of BAIC systems for financial e-governance services to highlight the significant enhancements achieved and the practical obstacles they faced. Using BAIC concepts and systems, distributed-branch banks recorded a significant reduction in time and cost for their overseas payments, while simultaneously achieving robustness against expected counterfeiting [53]. In addition, some hospitals and cosmetic and healthcare centers adopted the BAIC combination to manage patient information securely, and they used AI capabilities in big data analysis to provide accurate diagnoses with significant treatment outcomes [62]. Such adoptions of BAIC systems indicate future enhancements and the potential utility of Blockchain systems supported by AI techniques. Additionally, this section provides a deeper exploration of scalability and the computational power required for BAIC systems. On the other hand, challenges are also discussed, such as the required infrastructure, high-capacity computing power, and additional AI capabilities that must be added to traditional Blockchain systems.

4.1. Secure-transaction enhancements

Integrating AI capabilities with financial Blockchain led to significantly greater improvements in transaction security. AI techniques such as machine learning (or Deep Learning) provide accurate, real-time detection of anomalous transactions by analyzing large datasets [7]. An extra level of protection is added to Blockchain ledgers by combining decentralization with AI techniques, which helps detect and block counterfeit transactions and prevent them from being authorized in the system. Table 2 demonstrates the performance achieved by applying the BAIC combination, with the results from ordinary Blockchain also listed. Table 2 relies on security performance as a criterion for measuring (or digitizing) system performance, with their differences explaining enhancements between the two systems.

Table 2. Enhancements yielded by BAIC combinations versus ordinary Blockchain systems

Financial Transaction	Ordinary Blockchain	BAIC
True Counterfeit Detection	69.84%	92.07%
False Counterfeit Detection	25.18%	9.95%
Detection Time	31.28 seconds	13.16 seconds
Yearly Intrusion Accidents	4	1

Table 2 shows that constructing a BAIC yields higher performance in counterfeit-transaction detection, a considerably lower false-detection rate, lower time consumption, and a significant reduction in the number of successful attacks. Generally, recent publications adopting BAIC systems have shown that this combination reduces processing time for completing a financial transaction by 40%; in the same context, operational costs were reduced by 30%, whereas error rates decreased by 25% [63]. Such results emphasize the efficiency of BAIC systems and justify the growing number of authors adopting it to improve their financial transaction performance.

4.2. Enhancements in transparency

The public ledger of traditional Blockchain is combined with real-time AI techniques to enhance transparency in Blockchain operations. Decentralization concepts in Blockchain emphasize recording all financial operations in an accessible ledger, where each involved node can trace its transactions, and there is no need for an intermediary node to access them. To enhance Blockchain transparency, AI techniques analyze and process all blockchain transactions simultaneously, which ensures that all information is accurate and dynamically updated. For example, BAIC systems can simultaneously monitor for unusual activity or Blockchain conflicts and indicate any transactions requiring further verification. Continuous monitoring provides strong assurance and trust in transaction data recorded on the blockchain by all parties, which is highly demanded for Blockchain transparency.

Fig. 4 depicts that integrating BAIC systems provides more transparency and higher security for blockchain transactions. It shows the triangular cooperation among transactions, AI enhancements, and secure Blockchain operations [64], where AI techniques capture, analyze, and process incoming data to make timely, accurate, and secure decisions. Such techniques leverage their ability to handle large volumes of data to enable real-time processing for highly accurate transaction monitoring. The triangular relationship among Blockchain security, AI techniques, and entry transactions forms a continuous cycle through which data is exchanged. In such cooperation, Blockchain nodes connect to form a robust network that resists fraudulent transactions and counterfeit entries.

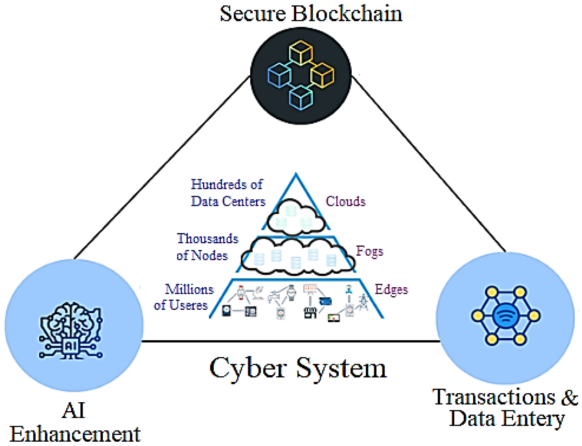

Fig. 4. Triangular relationship in BAIC systems to ensure secure transactions

4.2.1. AI techniques and smart contracts

In common situations, most financial institutions rely on AI-based smart contracts on Blockchain platforms to automate and verify financial agreements. Such contracts use smart contracts and are programmed to execute automatically upon preset conditions; meanwhile, AI techniques monitor preset security conditions and verify that they are met. Such an auto-process eliminates the need for an intermediary, thereby reducing transaction processing time and costs. Whereas contract conditions are stored as Blockchain records, each node on the network can easily verify agreement status, ensuring that the entire process is auditable and transparent [5]. A summary of published results illustrated that processing time recorded a decrement by about (40%) regarding financial contracts and an increment by about (30%) regarding user satisfaction, where different users noticed higher Blockchain efficiency and transparency.

4.2.2. BAIC combination in principal banks

In another application of BAIC, global banks successfully integrated BAIC for counterfeit detection to increase transaction security, especially across international records [65]. In ordinary Blockchain systems, such banks have faced several instances of counterfeit transactions, especially in international payments. Using BAIC systems, successful banks controlled, monitored, and analyzed such payments in real time and flagged all suspicious activities for further inspection. Adopting traditional Blockchain systems ensures that, by verifying a transaction as a record, it is shared on a decentralized ledger without the ability to manipulate it. The Islamic Bank in Iraq adopted BAIC-enhanced Blockchain for international payments and financial transactions, reducing the risk of forgery and errors, improving security indicators, and streamlining financial processes [66].

In the same context, medical Blockchain systems were used to digitize a patient's medical information to create an Electronic Medical Record (EMR), which various hospitals and medical companies adopted to leverage BAIC systems for cost reduction, traceability, and data accuracy [67]. Such adoption cases highlight the significant utility of BAIC integration, with recorded forgery decrements exceeding 55%. On the other hand, verification efficiency for BAIC-based banks increased significantly, with verification time reduced to half of the standard Blockchain verification time (on average). In addition, adopting BAIC integration provided greater transparency, enabling them to track their international transactions overall and exchange [68].

4.2.3. Administrative effects

Integrating BAIC systems showed significant benefits, with enhanced Blockchain systems powered by AI techniques and algorithms providing considerable improvements in transparency, stability, and security for all financial transactions [26, 69]. Real-time detection of counterfeit transactions was enabled by AI techniques, combined with anomaly identification and anticipatory analysis, to help financial institutions proactively manage expected risks. On the other hand, this is supported by Blockchains, which provide a decentralized, immutable ledger for transparent, integrated transactions [5]. A BAIC combination then creates a sturdy defense against security challenges facing a financial administration, ensuring efficient and reliable transactions. Practical case studies provided by industrial administrations showed that implementing BAIC integration reduced counterfeit transactions, simplified record verification, and ensured compliance with legislative standards. This situation provides BAIC integration as an inter-stage development in the global financial field [53, 70].

The financial administration perspective presents this review from different critical perspectives in the financial field. The integration of BAIC systems requires holistic support for Blockchain protocols to enable pre-detection of expected attacks. Administrations have all the motivation to analyze anticipated technologies to support Blockchain efficiency, as well as compliance with legislation, strict standards, and transparency to ensure transaction integrity [53]. Furthermore, integrating BAIC systems encourages cultural innovation, requiring administrations to update their strategies regularly to keep pace with evolving challenges. For future suggestions, researchers are encouraged to propose dynamic solutions to meet broader demands.

4.3.4. Research gap in previous works

Despite the considerable achievements, previous works still have some limitations. Firstly, they relied on published articles and empirical evidence to treat financial transactions as fully secure operations. They lacked questioning about the possibility of recording data under incorrect or falsified conditions. On the other hand, forged data may be injected into ledgers by data network participants or intruders, affecting Blockchain security and transparency. Such situations provide significant opportunities for future work. In addition, although all BAIC transactions are transparent, secured, and decentralized, the possibility of data hacking must still be considered. Thus, this review suggests that more attention should be paid to security issues (especially privacy protection), since absolute security can occur only in idealized, theoretical cases.

5. Conclusions

This review paper presented a comprehensive discussion of published papers in the field of Blockchain systems and their support with Artificial Intelligence (AI) techniques to form Blockchain-AI Combination (BAIC). Combining BAIC systems has raised significant expectations for the development of e-governance financial transactions in terms of transparency, stability, and security. AI techniques contribute to transaction security by enabling real-time counterfeit detection, pre-analysis, and the identification of unauthorized attacks, thereby creating a robust system for financial institutions against expected risks. On the other hand, Blockchain systems provided a decentralized, immutable ledger that enhances transaction transparency and integrity. Such a combination of BAIC builds robust Blockchain systems that address security challenges widely faced by traditional e-governance systems in the financial sector and provide reliable, effective solutions.

Implementing BAIC systems for e-governance-based institutions is crucial, efficient, and supportive. Supporting Blockchain systems with AI techniques increases the processing capabilities of data exchanged across Blockchain nodes. This is accomplished through a secure institution's infrastructure to reduce counterfeit transaction rates, reduce resource consumption for transaction verification, and support compliance with legislative requirements. Furthermore, BAIC combination integration simplifies processes, reduces the need for intermediaries, and decreases operational costs. Scientific papers, industrial reports, and Case studies discussed by this review indicated how BAIC-based institutions benefit from significant enhancements in transaction transparency and security. This demonstrated the holistic expectations of BAIC combinations for supporting e-governance systems.

With clear benefits, a wide range of challenges is still expected, especially regarding computational demands, scalability, and legislation changes. Implementing BAIC solutions requires a significant investment to ensure suitable infrastructure and compatibility with legislation. For future suggestions, researchers are advised to focus on developing adaptive solutions to create enhanced frameworks suitable for broader development. In general, integrating BAIC systems presents an encouraging roadmap for building a higher-security, more transparent e-governance framework, achieving future targets for economic enhancements and greater system transparency.

Acknowledgment

The authors of this paper would like to acknowledge the Middle Technical University and Jordan University and the productive cooperation between them, which enabled us to produce this review.

References

[1] Bathula et al., "Blockchain, artificial intelligence, and healthcare: the tripod of future—a narrative review," Artif. Intell. Rev., vol. 57, no. 9, p. 238, 2024, doi: 10.1007/s10462-024-10873-5.

[2] E. Badidi, "Edge AI and Blockchain for Smart Sustainable Cities: Promise and Potential," 2022. doi: 10.3390/su14137609.

[3] H. Omidian, "Synergizing blockchain and artificial intelligence to enhance healthcare," Drug Discov. Today, vol. 29, no. 9, p. 104111, 2024, doi: 10.1016/j.drudis.2024.104111.

[4] V. El Ardeliya, J. Taylor, and J. Wolfson, "Exploration of Artificial Intelligence in Creative Fields: Generative Art, Music, and Design," Int. J. Cyber IT Serv. Manag., vol. 4, no. 1, pp. 40–46, 2024, doi: 10.34306/ijcitsm.v4i1.149.

[5] D. Ressi, R. Romanello, C. Piazza, and S. Rossi, "AI-enhanced blockchain technology: A review of advancements and opportunities," J. Netw. Comput. Appl., vol. 225, p. 103858, 2024, doi: 10.1016/j.jnca.2024.103858.

[6] Shabnam Sharmin and Rakibul Hasan Chowdhury, "Digital Transformation in Governance: The Impact of e-governance on Public Administration and Transparency," J. Comput. Sci. Technol. Stud., vol. 7, no. 1, pp. 362–379, 2025, doi: 10.32996/jcsts.2025.7.1.27.

[7] M. Paramesha, N. Rane, and J. Rane, "Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: a comprehensive review," SSRN Electron. J., 2024, doi: 10.2139/ssrn.4855893.

[8] D. Hawashin et al., "Blockchain applications in UAV industry: Review, opportunities, and challenges," J. Netw. Comput. Appl., vol. 230, p. 103932, 2024, doi: 10.1016/j.jnca.2024.103932.

[9] Z. Abbas, F. A. Abed, N. J. Alhyani, and M. F. Mosleh, "Performance Enhancements of the Indoor Localization System Based on Dynamic ToA and RSS Mechanisms," in Lecture Notes in Networks and Systems, Springer, 2022, pp. 521–532. doi: 10.1007/978-3-030-85990-9_42.

[10] M. R. Anwar and L. D. Sakti, "Integrating Artificial Intelligence and Environmental Science for Sustainable Urban Planning," IAIC Trans. Sustain. Digit. Innov., vol. 5, no. 2, pp. 179–191, 2024, doi: 10.34306/itsdi.v5i2.666.

[11] K. Ulrich, J. M. Guaita Martínez, P. Carracedo, and D. R. Soriano, "Blockchain technology-based crypto assets: new insights into the evolution of the understanding of digital entrepreneurship," Manag. Decis., vol. 62, no. 9, pp. 2836–2854, 2024, doi: 10.1108/MD-03-2023-0306.

[12] M. Agarwal, K. S. Gill, D. Upadhyay, S. Dangi, and K. R. Chythanya, "The Evolution of Cryptocurrencies: Analysis of Bitcoin, Ethereum, BitConnect, and Dogecoin in Comparison," in 2024 IEEE 9th International Conference for Convergence in Technology, I2CT 2024, IEEE, 2024, pp. 1–6. doi: 10.1109/I2CT61223.2024.10543872.

[13] K. Tyagi, S. Dananjayan, D. Agarwal, and H. F. Thariq Ahmed, "Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0," Sensors, vol. 23, no. 2, p. 947, 2023, doi: 10.3390/s23020947

[14] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique, "Blockchain Application in Healthcare Systems: A Review," Systems, vol. 11, no. 1, p. 38, 2023, doi: 10.3390/systems11010038.

[15] M. S. Mutar, Z. A. Hamza, D. A. Hammood, and S. A. Hashem, "A survey of sleep scheduling techniques in wireless sensor networks for maximizing energy efficiency," in AIP Conference Proceedings, AIP Publishing LLC, 2024, p. 20058. doi: 10.1063/5.0236138.

[16] V. Sethaput and S. Innet, "Blockchain application for central bank digital currencies (CBDC)," Cluster Comput., vol. 26, no. 4, pp. 2183–2197, 2023, doi: 10.1007/s10586-022-03962-z.

[17] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer, 2016, pp. 112–125. doi: 10.1007/978-3-319-39028-4_9.

[18] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," IEEE Trans. Knowl. Data Eng., vol. 30, no. 7, pp. 1366–1385, 2018, doi: 10.1109/TKDE.2017.2781227.

[19] M. Kassen, "Blockchain and digital governance: Decentralization of decision making policy," Rev. Policy Res., vol. 42, no. 1, pp. 95–121, 2025, doi: 10.1111/ropr.12585.

[20] M. J. Fadhil, M. A. Naji, and G. A. Salman, "Transceiver error reduction by design prototype system based on neural network analysis method," Indones. J. Electr. Eng. Comput. Sci., vol. 18, no. 3, pp. 1244–1251, 2020, doi: 10.11591/ijeecs.v18.i3.pp1244-1251.

[21] G. Mustafa, W. Rafiq, N. Jhamat, Z. Arshad, and F. A. Rana, "Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations," Int. J. Law Manag., vol. 67, no. 1, pp. 37–55, 2025, doi: 10.1108/IJLMA-08-2023-0172.

[22] Z. Chen, S. E. Celik, and J. Sarkis, "A systematic review of academic literature for blockchain application in government and public service," J. Enterp. Inf. Manag., pp. 1–29, 2025, doi: 10.1108/JEIM-03-2024-0150.

[23] Z. Wang, X. Xiong, and W. J. Knottenbelt, "Blockchain Transaction Censorship: (In)secure and (In)efficient?," in The International Conference on Mathematical Research for Blockchain Economy, Springer, 2023, pp. 78–94. doi: 10.1007/978-3-031-48731-6_5.

[24] W. Liang, Y. Liu, C. Yang, S. Xie, K. Li, and W. Susilo, "On Identity, Transaction, and Smart Contract Privacy on Permissioned and

Permissionless Blockchain: A Comprehensive Survey," ACM Comput. Surv., vol. 56, no. 12, pp. 1–35, 2024, doi: 10.1145/3676164.
[25] Wahrstätter et al., "Blockchain Censorship," in WWW 2024 - Proceedings of the ACM Web Conference, 2024, pp. 1632–1643. doi: 10.1145/3589334.3645431
[26] Gopalan, A. Sankararaman, A. Walid, and S. Vishwanath, "Stability and Scalability of Blockchain Systems," Perform. Eval. Rev., vol. 48, no. 1, pp. 71–72, 2020, doi: 10.1145/3393691.3394218.
[27] Q. Deng, Q. Zuo, Z. Li, H. Liu, and Y. Xie, "Privacy-Preserving Stable Data Trading for Unknown Market Based on Blockchain," IEEE Trans. Mob. Comput., vol. 24, no. 7, pp. 5615–5631, 2025, doi: 10.1109/TMC.2025.3534201.
[28] M. Anjali, S. A. Vali, J. Divya, and B. Lokesh, "A Next-Generation Blockchain Framework for Secure and Tamper-Proof Online Examinations," in Proceedings of the International Conference on Intelligent Computing and Control Systems, ICICCS 2025, IEEE, 2025, pp. 615–622. doi: 10.1109/ICICCS65191.2025.10985063.
[29] J. Kadhim and G. A. Salman, "Secure archiving system: Integrating object information with document images using mathematical coding techniques," in AIP Conference Proceedings, AIP Publishing LLC, 2024, p. 20048. doi: 10.1063/5.0236296.
[30] Rakibul Hasan Chowdhury, "Blockchain and AI: Driving the future of data security and business intelligence," World J. Adv. Res. Rev., vol. 23, no. 1, pp. 2559–2570, 2024, doi: 10.30574/wjarr.2024.23.1.2273.
[31] Krittanawong et al., "Integrating blockchain technology with artificial intelligence for cardiovascular medicine," Nat. Rev. Cardiol., vol. 17, no. 1, pp. 1–3, 2020, doi: 10.1038/s41569-019-0294-y.
[32] N. Andola, Raghav, V. K. Yadav, S. Venkatesan, and S. Verma, "Anonymity on blockchain based e-cash protocols - A survey," Comput. Sci. Rev., vol. 40, p. 100394, 2021, doi: 10.1016/j.cosrev.2021.100394.
[33] E. Oye, S. Williams, and G. Taylor, "Blockchain Anonymity and the Challenges of Detecting Illicit Financial Flows," 2025.
[34] M.-A. Preprints and undefined 2025, "Blockchain-Driven Cybersecurity Audits: Securing Financial Systems with Trust and Transparency," Authorea.Com, 2025, [Online]. Available: https://www.authorea.com/doi/full/10.22541/au.173862082.22380043
[35] Kadhim, F. Mohamed, F. H. Najjar, G. A. Salman, and A. J. Ramadhan, "Localizing the Thickness of Cortical Regions to Descriptor the Vital Factors for Alzheimer's Disease Using UNET Deep Learning," in BIO Web of Conferences, EDP Sciences, 2024, p. 54. doi: 10.1051/bioconf/20249700054.
[36] M. A. Naji, G. A. Salman, and M. J. Fadhil, "Face recognition using selected topographical features," Int. J. Electr. Comput. Eng., vol. 10, no. 5, pp. 4695–4700, 2020, doi: 10.11591/ijece.v10i5.pp4695-4700.
[37] G. A. Salman and N. F. Hasan, "Analyzing the Differences of Female/ Male Faces on Recognition Accuracy," in 2022 Iraqi International Conference on Communication and Information Technologies, IICCIT 2022, IEEE, 2022, pp. 107–113. doi: 10.1109/IICCIT55816.2022.10010416.
[38] G. A. Salman and N. F. Hasan, "Designing deep learning neural network for auto-detection of growing weeds within grass lands," in AIP Conference Proceedings, AIP Publishing, 2023. doi: 10.1063/5.0155761.
[39] Waqar, "Intelligent decision support systems in construction engineering: An artificial intelligence and machine learning approaches," Expert Syst. Appl., vol. 249, p. 123503, 2024, doi: 10.1016/j.eswa.2024.123503
[40] S. Kusuma Kumar Parimi, "Adaptation and Learning in AI Agents," Int. J. Sci. Res. Eng. Manag., vol. 09, no. 04, pp. 1–9, 2025, doi: 10.55041/ijsrem45372.
[41] S. K. Singh, S. Kumar, and P. S. Mehra, "Chat GPT and Google Bard AI: A Review," in 2023 International Conference on IoT, Communication and Automation Technology, ICICAT 2023, IEEE, 2023, pp. 1–6. doi: 10.1109/ICICAT57735.2023.10263706.
[42] X. Zhang, P. Yu, L. Ma, and Y. Liang, "How the human-like characteristics of AI assistants affect employee creativity: a social network ties perspective," Int. J. Human–Computer Interact., vol. 41, no. 10, pp. 6431–6449, 2025.
[43] Y. Zhou, M. Zhang, Y. J. Zhu, and Q. Lu, "Research progress on the application of deep learning in choroidal segmentation," Int. Eye Sci., vol. 23, no. 6, pp. 1007–1011, 2023, doi: 10.3980/j.issn.1672-5123.2023.6.25.
[44] T. K. Ng, M. Lee, R. J. Y. Tan, X. Hu, J. S. Downie, and S. K. W. Chu, "A review of AI teaching and learning from 2000 to 2020," Educ. Inf. Technol., vol. 28, no. 7, pp. 8445–8501, 2023, doi: 10.1007/s10639-022-11491-w.
[45] M. H. Mohd Noor and A. O. Ige, "A survey on state-of-the-art deep learning applications and challenges," Eng. Appl. Artif. Intell., vol. 159, p. 111225, 2025, doi: 10.1016/j.engappai.2025.111225.
[46] S. Gao, Z. Lu, H. Luan, M. Yin, and L. Wang, "AI Pilot in the Cockpit: An Investigation of Public Acceptance," Int. J. Hum. Comput. Interact., vol. 41, no. 1, pp. 543–556, 2025, doi: 10.1080/10447318.2024.2301856.
[47] Wenjing, "Simulation application of virtual robots and artificial intelligence based on deep learning in enterprise financial systems," Entertain. Comput., vol. 52, p. 100772, 2025, doi: 10.1016/j.entcom.2024.100772.
[48] Cai et al., "The Role of Deductive and Inductive Reasoning in Large Language Models," in Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), 2025, pp. 16780–16790. doi: 10.18653/v1/2025.acl-long.820.
[49] M. A. S. G, N. V, and R. J. Lontok, "Object Identification and Classification from Thermal Images Using the Ensemble Learning Across Various YOLO Models," in Lecture Notes on Data Engineering and Communications Technologies, Springer, 2025, pp. 178–193. doi: 10.1007/978-3-031-91354-9_15.
[50] Jamieson, C. F. Moreno-Garcia, and E. Elyan, "Towards fully automated processing and analysis of construction diagrams: AI-powered symbol detection," Int. J. Doc. Anal. Recognit., vol. 28, no. 1, pp. 71–84, 2025, doi: 10.1007/s10032-024-00492-9.
[51] Ghalib Ahmed Salman, Inas Jawad Kadhim, and Ahmed Husham Al-Badri, "Image-Based Face Recognition Techniques Used in Disease Detection Approaches: A Survey," J. Tech., vol. 6, no. 1, pp. 33–44, 2024, doi: 10.51173/jt.v6i1.1966.
[52] Z. Chen, S. E. Celik, and J. Sarkis, "A systematic review of academic literature for blockchain application in government and public service," J. Enterp. Inf. Manag., vol. 39, no. 1, pp. 1–29, 2025, doi: 10.1108/JEIM-03-2024-0150.
[53] U. Sadyk, R. Baimukashev, and C. Turan, "State-of-the-Art Review of Deep Learning Methods in Fake Banknote Recognition Problem," Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 1, pp. 848–856, 2024, doi: 10.14569/IJACSA.2024.0150185.
[54] Mohammad, S. Vargas, and P. Čermák, "Using Blockchain for Data Collection in the Automotive Industry Sector: A Literature Review," J. Cybersecurity Priv., vol. 2, no. 2, pp. 257–275, 2022, doi: 10.3390/jcp2020014
[55] Ivey and J. Crum, "Choosing the right citation management tool: EndNote, Mendeley, RefWorks, or Zotero," J. Med. Libr. Assoc., vol. 106, no. 3, p. 399, 2018, doi: 10.5195/jmla.2018.468
[56] N. Gariya, A. Asrani, A. Mandal, A. Shaikh, and D. Cha, "A Comprehensive Analysis of Integrating Blockchain Technology into the Energy Supply Chain for the Enhancement of Transparency and Sustainability," Energies, vol. 18, no. 11, p. 2951, 2025, doi:

10.3390/en18112951.
[57] R. W. Ahmad, K. M. Ko, A. Rashid, and J. J. P. C. Rodrigues, “Blockchain for Food Industry: Opportunities, Requirements, Case Studies, and Research Challenges,” IEEE Access, vol. 12, pp. 117363–117378, 2024, doi: 10.1109/ACCESS.2024.3447918.
[58] A. Alaoui and H. Azdimousa, “The Combination of AI and Blockchain for Impact Investing,” in Lecture Notes in Networks and Systems, Springer, 2025, pp. 766–774. doi: 10.1007/978-3-031-91334-1_68
[59] A. Ahmed and O. O. Alabi, “Secure and Scalable Blockchain-Based Federated Learning for Cryptocurrency Fraud Detection: A Systematic Review,” IEEE Access, vol. 12, pp. 102219–102241, 2024, doi: 10.1109/ACCESS.2024.3429205.
[60] G. A. Salman, A. S. Arif, and S. Mansor, “Corresponding Influence of Gender variation and Age Progression on Result Performance of Each Other,” in 2025 Multimedia University Engineering Conference (MECON), IEEE, 2025, pp. 1–5. doi: 10.1109/MECON67253.2025.11276967.
[61] R. U. Khan, K. Ullah, and M. Atiq, “Regulatory constraints, responsibilities and consultation (CRC) for legal institutionalization of cryptocurrencies in Pakistan,” Qual. Res. Financ. Mark., vol. 16, no. 4, pp. 680–708, 2024, doi: 10.1108/QRFM-03-2023-0053.
[62] S. A. Shammi, P. Ghosh, A. Sutradhar, F. M. J. M. Shamrat, M. A. Moni, and T. E. A. De Oliveira, “Advances in Artificial Intelligence and Blockchain Technologies for Early Detection of Human Diseases,” IEEE Trans. Comput. Soc. Syst., vol. 12, no. 1, pp. 210–237, 2025, doi: 10.1109/TCSS.2024.3449748.
[63] Martinez, L. Magdalena, and A. N. Savitri, “AI and Blockchain Integration: Enhancing Security and Transparency in Financial Transactions,” Int. Trans. Artif. Intell., vol. 3, no. 1, pp. 11–20, 2024, doi: 10.33050/italic.v3i1.651.
[64] Tauseef, M. R. Kounte, A. H. Nalband, and M. R. Ahmed, “Exploring the Joint Potential of Blockchain and AI for Securing Internet of Things,” Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 4, pp. 885–895, 2023, doi: 10.14569/IJACSA.2023.0140498.
[65] Begum, M. S. K. Munira, and S. Juthi, “Systematic Review of Blockchain Technology in Trade Finance and Banking Security,” Am. J. Sch. Res. Innov., vol. 1, no. 01, pp. 25–52, 2022, doi: 10.63125/vs65vx40
[66] J. Alhchaimi and ..., “Islamic Finance and Digital Currencies: An Overview The development of Blockchain adoption in Iraq and Arab countries.,” J. Univesity Thi …, vol. 20, no. 2, pp. 177–196, 2025.
[67] J. Al-Jaroodi and N. Mohamed, “Blockchain in Industries: A Survey,” IEEE Access, vol. 7, pp. 36500–36515, 2019, doi: 10.1109/ACCESS.2019.2903554.
[68] S. M. M. Rahman, K. J. Yii, E. K. Masli, and M. L. Voon, “The blockchain in the banking industry: a systematic review and bibliometric analysis,” Cogent Bus. Manag., vol. 11, no. 1, p. 2407681, 2024, doi: 10.1080/23311975.2024.2407681.
[69] P. A. D. S. N. Wijesekara, “A Review of Blockchain-Rooted Energy Administration in Networking,” Indones. J. Comput. Sci., vol. 13, no. 2, 2024, doi: 10.33022/ijcs.v13i2.3818.
[70] Z. Halász, “The Development of Crypto Legislation in Europe,” Hungarian Yearb. Int. Law Eur. Law 2024, vol. 12, no. 1, pp. 439–456, 2024, doi: 10.5771/9783748946526-439.