

Blockchain and Artificial Intelligence Integration: A Review of Applications, Challenges, and Future Directions

Areej Mahmoud Asaad^{1,*} , Mahmood Hameed Qahtan² , Ahmed Kh. Younis³ 



^{1,3} Department of Computer Techniques Engineering, Technical Engineering College for Computer and Artificial Intelligence, Mosul, Northern Technical University, Mosul 41001, Iraq.

² Department of Artificial Intelligence Techniques Engineering, Technical Engineering College for Computer and Artificial Intelligence, Mosul, Northern Technical University, Mosul 41001, Iraq.

*Correspondence: areej_mahmoud@ntu.edu.iq

Abstract: Blockchain and AI were developed separately, but nowadays, there is research on the integration of those technologies to benefit from both. First, the blockchain technology gives such possibilities as data provenance, decentralized trust, and tampering resistance; second, the artificial intelligence gives prediction possibilities and algorithms for making decisions. Literature review about the research which has been done in 2026 concerns the combination of blockchain and AI in the following fields: health care, financial industry, logistics, energy sector, smart cities, and decentralized training using AI. Advantages connected with security, data integrity, privacy, and efficiency, as well as possible barriers associated with scalability, computational costs, quality of data, and regulation are mentioned in the review. The review shows that blockchain may increase security and trust in AI systems, while AI may increase efficiency of blockchain systems. The possible trends include lightweight inference, privacy-preserving machine learning, and AI-based smart contracts security.

Keywords: blockchain; artificial intelligence; federated learning; smart contracts; decentralized systems; data privacy.

Review – Peer Reviewed

Received: July 30, 2026

Accepted: September 16, 2026

Published: September 27, 2026

Copyright: © 2026 RAME Publishers

This is an open access article under the CC BY 4.0 International License.



<https://creativecommons.org/licenses/by/4.0/>

Cite this article: Areej Mahmoud Asaad, Mahmood Hameed Qahtan, Ahmed Kh. Younis, "Blockchain and Artificial Intelligence Integration: A Review of Applications, Challenges, and Future Directions", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 7, issue 4, pp. 498-511, 2026.

<https://doi.org/10.26706/ijceae.7.4.20260815>

1. Introduction

While blockchain started as a ledger technology supporting Bitcoin, it is now seen as an adaptable platform that allows for decentralization and immutability of information as well as programmed cooperation through smart contracts[1]. In contrast to blockchain, the technologies of artificial intelligence (including machine learning, deep learning, and reinforcement learning) have been seen as tools for pattern recognition and automation of decision-making processes. While emerging from different areas of scientific investigation, the recent progress in both fields shows that they can be increasingly viewed as supplementary technologies rather than rivals. This is because blockchain offers higher levels of trust, verification, and decentralization that are often missing in AI technologies, while AI offers adaptability and prediction capabilities that regular blockchain does not possess[2][3]. However, interest in the convergence of these technologies has skyrocketed in the last couple of years. According to recent systematic reviews, there have been more than a hundred peer-reviewed studies about the convergence of blockchain technology and AI in topics including security, financial applications, health care, energy, and smart cities [4][5]. This review makes use of the literature mentioned to provide a brief, applied approach overview. This is useful for people who want to have an initial understanding of the subject matter before going to more detailed studies. Section two covers past research concerning the combination of blockchain technology and artificial intelligence. Section three, meanwhile, covers the nature of the two technologies' synergy. Section four covers

six applications, and section five covers common technical and governance issues. Section six covers future research directions, and the last section covers the paper's conclusion.

1.1. Background and Fundamentals

1.1.1 Blockchain Fundamentals

The term Blockchain technology is defined as a decentralized database in which transactions take place between various nodes without any centralized authority [6]. Blockchain technologies use distributed ledgers, cryptography, and consensus algorithms like proof-of-work and proof-of-stake for validating the transactions and maintaining a common state [7]. Smart contracts refer to computer programs which are run on top of the blockchain and run predetermined tasks automatically upon meeting certain criteria. In a blockchain-AI environment, smart contracts can handle transactions related to AI applications, impose access control policies, and validate the results of the computations [8]. On the other hand, running resource-intensive AI inference on the blockchain is likely to incur delays and high transaction fees. As a solution, the use of Layer-2 technologies and off-chain computations can help conduct AI inference operations on the blockchain while validating the results cryptographically [9]. One approach is the implementation of zero knowledge proof (ZKP) protocols, wherein a prover can verify the correctness of a computation or a statement without revealing any of the underlying data. In the case of zkML approach, a proof can be created for an AI inference done off-chain and then validated on-chain using smart contracts. This will help the blockchain in validating the result without executing the whole AI model itself. But it is necessary to keep in mind the overhead in creating the proof and latency in verification [10]. Optimistic Rollups provide a layer-2 approach where computations are mostly done off-chain, and their outcomes are uploaded onto the blockchain. There are ways to challenge any incorrect result under this system. Hence, while deciding between ZKP verification and optimistic methods, one needs to weigh factors like computational overheads, verification latency, gas cost, privacy, and security [11].

1.1.2 AI Fundamentals

In artificial intelligence, there are several techniques that allow systems to learn, predict, reason and adapt. Machine Learning is used for making a system learn through data, whereas Deep Learning uses multilayered neural networks to represent data[12][13]. Federated Learning is another technique that enables the training of a shared machine learning model without sending data. Autonomous agents are capable of perception, reasoning, and acting toward their objectives using effective data pipelines[14].

1.1.3 Blockchain–AI Interplay

The combination of Blockchain and Artificial Intelligence (AI) results in a complementary paradigm where one technology can compensate for some deficiencies of another technology. The benefits that AI can bring to blockchain include smart-contract analysis with the use of machine intelligence, anomaly and fraud detection, security monitoring, and consensus optimization. At the same time, blockchain can help to increase the security, privacy, and trust of collaborative AI applications. In particular, combining blockchain and federated learning can provide additional security, privacy, and trust to collaborative AI. Consequently, this convergence of technologies serves as a basis for creating secure, trustworthy, and decentralized intelligent systems [15][16]. Considering the described complementary role of both technologies, the integration of Blockchain and AI can be divided into three main directions – AI for Blockchain, Blockchain for AI, and Blockchain + AI [17], as shown in Table 1.

Table 1. Taxonomy of Blockchain–AI Integration: Blockchain for AI, AI for Blockchain

Direction	Concept	Examples
AI for Blockchain	Using AI to enhance blockchain performance, security, and decision-making	Smart-contract security, consensus optimization, anomaly detection
Blockchain for AI	Using blockchain to address trust, privacy, integrity, and ownership challenges in AI	Data provenance, privacy, decentralized computing, model ownership
Blockchain + AI	Mutual integration of both technologies to develop secure and trustworthy intelligent systems	Secure intelligent systems, trustworthy AI, decentralized AI

2. Previous Studies: Blockchain and AI Integration (2026)

Recent studies show that combining blockchain and artificial intelligence (AI) enhances trust, transparency, and security through blockchain, while AI provides prediction and optimization[18]. Table 2 presents a selection of the literature, including areas of application, objectives, research gaps, traditional solutions, and implementation issues.

In 2026, Veerapaneni and Delhibabu [19] suggested a trustworthy intelligent room with blockchain based on Distributed Ledger Technology (DLT), Federated Learning (FL), and Data-Centric AI to support reliable healthcare. The proposed architecture was evaluated using a fall-detection case study. Data-Centric FL achieved $91.5\% \pm 0.9\%$ accuracy and an F1-score of 0.89 ± 0.01 , compared with $84.2\% \pm 1.4\%$ accuracy and an F1-score of 0.81 ± 0.02 for standard FL. The improvements were statistically significant, with $p < 0.001$ for accuracy and $p < 0.005$ for F1-score. In addition, under a poisoning attack, standard FL accuracy decreased from 91.2% to 76.5%, whereas the proposed DLT-based recovery approach achieved 89.8% accuracy and a fall-detection recall of 93.5%, compared with 62.1% for standard FL under attack. The proposed approach also recovered the system within approximately 3 s (one federated-learning round), demonstrating the potential of combining blockchain, FL, and Data-Centric AI to improve model reliability, accountability, and resilience against malicious updates.

The bibliometric analysis was performed by Bulut [20] in 2026 to examine the global trends and innovations concerning the use of artificial intelligence (AI) technologies in smart cities. In total, 810 papers published between 2004 and 2025 were considered and retrieved from the Web of Science database. These publications consisted of 2,815 authors, 1,405 organizations, 92 countries, and 87 journals. It also includes the analysis of co-authorship networks, co-citations, bibliographic couplings, and keywords with the use of the VOSviewer software. As a result, this research demonstrates the significant growth of the number of publications on the application of AI technology in smart cities after 2019. The maximum number of publications in this field is equal to 181 and was observed in 2024. Six major topics were defined: AI and machine learning, IOT, data security and blockchain, sustainability, and digital twins in urban planning.

The study conducted by Arshadi and Dombrowski [21] in 2026 looked at the implementation and management of blockchain technology in financial services, particularly in payment systems, wealth management, real estate, and corporate governance. Through an adjustment to the present value model using U.S. ACH data, comparative institutional analysis, and evidence from empirical studies, they found that blockchain real-time settlement can bring annual opportunity cost savings of about \$12 billion, with sensitivity estimates ranging from \$8 billion to \$15 billion. It is also found that there is great potential for blockchain, smart contracts, and tokenization to reduce intermediation costs and improve efficiencies, yet the governance of DAOs poses some challenges, such as Gini coefficient above 0.98 and voter turnout less than 10%.

Muhammad Iqbal et al. (2026) [22] presented a study aimed at reducing religious extremism and polarization among university students through an integrated framework utilizing artificial intelligence, the Internet of Things, blockchain technology, and cognitive science. Employing a six-phase R&D methodology, the study demonstrated that the AI natural language processing module achieved 94% precision and 89% recall. Additionally, cognitive behavioral therapy (CBT) interventions resulted in a 28% increase in tolerance scores ($p < 0.01$) and a 40% reduction in high-risk digital interactions. These findings suggest that combining these technologies with cognitive approaches can effectively address extremism and polarization beyond traditional methods.

Divya Upadhyay, Puneet Garg, and Nandini Babbar [23] put forward a B-IoT (blockchain, IoT, and smart contract) framework for improving product lifecycle management in 2026. In the said framework, purchase orders, invoices, and end-of-life processes have been automated using IoT and smart contract technology. According to the pilot study findings, accuracy and efficiency stood around 95% and 92%, respectively, increasing efficiency while decreasing the need for manual verification of processes. A research issue that exists is the lack of industrial-level testing of the framework concerning its scalability, reaction time, cost of implementation, and performance.

In 2026, B. S. Liya, Er. Harish Kumar, Mostake Md. Morshedur Hassan et al. [24] suggested a study that focuses on creating a secure and efficient architecture of controlling microgrids based on renewable energy with the help of edge-AI, IoT, and blockchain technology. For fault detection and optimization of control, Spiking Neural Networks were used while power transactions and access control were checked with the help of Hyperledger Fabric. The research revealed that Cyber Fault Detection Accuracy (CFDA) was 97.6%, with consensus time being below 2.3 seconds and voltage deviation $\pm 1.1\%$. Moreover, a decrease in communication overhead of 28% was attained as opposed to centralized control.

In 2026, Ruihua Bai [25] proposed a framework using blockchain, artificial intelligence, Internet of Things (IoT) and knowledge management to forecast potential contamination in food logistic. The model utilizes data from cold chain IoT devices and data about shipments. For this purpose, LSTM, Transformer and a physics-inspired hybrid approach were used, as well as unit learning to secure the data privacy. To build an immutable audit trail, Hyperledger Fabric was applied. The experiments demonstrated superior performance of the hybrid model, which showed PR-AUC = 0.945, Recall = 0.864 at 90% accuracy, with Brier Score = 0.058 and ECE = 0.013. In comparison, FedAvg and FedProx showed PR-AUC scores of 0.923 and 0.931 respectively, in contrast to 0.945 in centralized training case, proving minor decline in performance but retaining almost all predictive power and the data privacy protection capabilities. The system was able to send alerts about 5 days before the simulated recall operations.

A case study was presented by Rakesh Pal [26] in 2026 where the main focus was on increasing the market reach of smallholder farmers using blockchain and artificial intelligence (AI). The proposed distributed system linked the identity and products of the farmers to reliable documents, where the use of blockchain helped in product tokenization and traceability and smart contracts performed all transactions automatically. Various AI technologies were used to predict prices, match buyers and products, categorize crops, and analyze risks. The study included 6–8 farmer's associations and about 1,200 farmers, and analyzed various parameters such as prices, payment periods, and rejection rates. The study revealed 8–12% improvement in farm gate prices, payment period reduced from T+7 to T+1-T+2, and rejection rate reduced from 9.4% to 5.1%.

In 2026, Malak Al-Omari et al. [27] presented an energy-efficient threat detection framework for IoT-based healthcare using artificial intelligence and blockchain in a fog-cloud framework. For the detection of attacks, the researchers used XGBoost, for model optimization, Smart AFSO, for imbalanced data, and SMOTE, and for creating an immutable audit log, blockchain technology was used. In the model, which consisted of various combinations of BoT-IoT and ToN-IoT, the achieved accuracy was 99.8%, and the F1-score was 98.7%, whereas the AUC and MCC were 1.00 and the block creation time was 10.11 ms. It was also observed that there was less execution time in the fog as compared to the cloud, where the execution times were 3.67 seconds and 7.68 seconds, respectively. However, the experiment was limited to a simulation environment, and the model had some shortcomings in coping with the problem of conceptual drift and adversarial attacks.

Khan et al. (2026) [28] suggested a framework that combines AI and blockchain technology. This framework is based on blockchain for decentralization and storing immutable logs, and a CNN-LSTM framework to help intelligently detect cyber attacks. With the use of CICIDS2017 dataset, and SMOTE to solve the problem of imbalanced datasets, this framework showed a 98.2% accuracy rate, classification precision of 97.6%, recall of 97.1%, and 97.3% F1 score. In addition, it recorded a false alarm rate of 1.8% and a detection time of about 3.2 milliseconds per sample. In its blockchain verification layer, the framework had a success rate of 99.1%, performing better than SVM, Random Forest, CNN, LSTM, and pure blockchain systems. Nonetheless, despite these amazing results, some limitations were noted from the study, as it was performed in private blockchain simulation.

The paper written by Gafsi, Hamdouni, and Smaoui (2026) [29] looked into the effect of digital innovations, including FinTech, artificial intelligence (AI), and Blockchain, on sustainable development in the economies of G20 countries during 2015–2023. Applying panel data and macroeconomic factors as controls, the research was based on Innovation-Driven Growth Theory, TOE models, and Institutional Theory. It was found that all of the technologies have a statistically significant positive effect on sustainable development (the coefficient is 0.327 for AI, 0.214 for FinTech, and 0.189 for Blockchain, significant at $p < 0.01$). It is worth noting that the combination of technologies brings more benefits to sustainable development compared to the evaluation of each technology separately.

The study by Adebiyi et al. (2026) [30] used a quantitative approach for the development of a B-AITTF framework, which is the combination of blockchain and AI technologies for improving the level of trust, transparency and compliance in cross-border finance. The methods included panel regression, logistic regression, SEM analysis, and Monte Carlo simulation; the data was taken from international financial databases and the Elliptic AML data set. The fraud detection system gave an accuracy of 90.1%; the suggested framework managed to decrease the average settlement time from 48.045 hours to 30.074 hours, increase the confidence coefficient from 0.621 to 0.801 and decrease the data lineage error from 0.035 to 0.015.

Gunjan Mishra and Yash Mishra (2026) [31] presented an Adaptive Neuro-Fuzzy Blockchain–AI framework (ANFB-AI) for improving the security of transactions. This architecture consists of a permissioned blockchain using a proof-of-authority algorithm along with machine learning models that analyze the risk of transactions. It was tested using 50,000 transactions through three fraud cases and achieved highly successful results: Accuracy 98.9%, Precision 98.9%, Recall

98.1%, F1-Score 98.5%, ROC-AUC 0.992, and MCC 0.972. The results from the ablation test have confirmed that ANFB-AI framework performs much better than the models without feedback from the blockchain. Moreover, it ensures low confirmation time of transactions despite a high amount of fraud.

An architecture to protect MRI images that are used in AI algorithms to detect brain tumors from any kind of tampering or data poisoning attacks was introduced by Shinde et al. (2026) [32]. In this regard, the authors developed the architecture by using the combination of Hyperledger Fabric and Private IPFS architectures. In the architecture, an authorized blockchain, role-based access control, and private datasets have been used. The MRI images have been stored off-blockchain, but CIDs along with other metadata have been stored on the blockchain. From the experiments done in Hyperledger Caliper, the framework was able to upload 42 images successfully with no failures, where operation per second was 1.8, and average response time was 1.49 seconds.

Stephen et al. (2026) [33] designed an integration framework which includes artificial intelligence, IoT and blockchain technology for coal waste management and recovery in the circular economy context. ResNet-50 model was used for the identification of coal waste from the images, and for the real-time collection of data, IoT technology was used. For storing the data regarding the waste processing and emission in a tamper-proof manner, Hyperledger Fabric was used. In the current study, smart contracts have been employed to automate the process of tracking and documenting the operations. As a result of validation done in 142 coal processing plants, the rate of classification accuracy has been found about 95%, energy savings about 34%, carbon dioxide emissions reduction by 30% and reduction in water pollution by 81%. The average blockchain transaction time was approximately 0.42 ± 0.05 seconds, and the system achieved a payback period of 3.6 years and a return on investment of 22%.

Table 2. Comparative Analysis of Blockchain–AI Integration Studies

References	Sector / Study Type	Usage	Gaps	Traditional Mitigation Methods	Notable Weaknesses in Traditional Methods	Prominent Applications of Blockchain and AI	Research and Dissemination Challenges
[19] Veerapaneni & Delhibabu (2026)	Healthcare 4.0 original research (smart/intelligent hospital rooms)	DLT-secured federated learning + data-centric AI for real-time ambient patient monitoring (fall detection) via Fog-Cloud architecture	Standard FL's central aggregator is a single point of failure vulnerable to poisoning; existing smart rooms lack interoperability and continuous learning	Centralized cloud AI diagnosis tools (e.g., VisualDX), wearable sensors, computer-vision bed monitoring, optical fall detectors (Kepler Night Nurse)	High latency; privacy risk; siloed, static systems	Blockchain-audited FL updates; smart-contract validation; data-centric AI	Poor consensus scalability; untested long-term drift
[20] Bulut (2026)	Smart Cities /Bibliometric Study	Bibliometric analysis of 810 WoS publications (2004–2025)	Limited standardization of data , AI governance, interdisciplinary collaboration	Centralized data, security, governance, and AI systems	Privacy and security risks, limited interoperability, data silos, and difficulty managing heterogeneous urban data.	Urban planning, IoT, security/trust, digital twins, environmental monitoring	Standardization, ethics, interoperability, integration, validation, and collaboration.
[21] Arshadi & Dombrowski (2026)	Financial Services – Analytical Review	Examines blockchain applications, governance, management, and adoption in financial services, including DeFi, smart contracts, and DAOs.	Regulatory uncertainty, limited governance understanding, scalability and interoperability issues, and limited empirical research on adoption.	Centralized banking, payment systems, intermediaries, databases, and conventional regulatory and risk-management mechanisms.	Centralization creates single points of failure, reduces transparency, increases intermediary dependence, and may raise costs.	Blockchain-based payments, DeFi, smart contracts, DAOs, secure transactions, and AI-based fraud detection, risk assessment, and prediction.	Regulatory uncertainty, scalability, interoperability, privacy, security, governance concentration, integration with existing infrastructure, and lack of standards.
[22] Muhammad Iqbal et al. (2026)	Education / AI–Blockchain Integration	Integrates AI, IoT, blockchain, and cognitive science to detect and mitigate religious radicalism and polarization in universities	Limited contextual AI detection, lack of real-time behavioral analysis, privacy concerns, and limited integrated prevention frameworks.	Offline seminars, religious counseling, punitive measures, and conventional deradicalization programs	Limited scalability and digital relevance; difficulty addressing online and cognitive mechanisms of radicalization	AI-based radical-content detection, IoT behavioral monitoring, blockchain- secured logging, and cognitive-behavioral interventions	False positives, privacy and surveillance concerns, ethical bias, cultural context, scalability, and need for cross-cultural and longitudinal validation.

References	Sector / Study Type	Usage	Gaps	Traditional Mitigation Methods	Notable Weaknesses in Traditional Methods	Prominent Applications of Blockchain and AI	Research and Dissemination Challenges
[23] Upadhyay, D., Garg, P., & Babbar, N. (2026)	Supply Chain and Product Lifecycle Management / Applied Framework Study	Blockchain–IoT smart contracts automate purchase orders, delivery invoicing, and product disposal after expiry.	Requires broader real-world and large-scale validation, particularly for scalability, transaction costs, execution time, and varying operational conditions	Centralized databases, manual verification, paper-based records, and centralized coordination for ordering, delivery, invoicing, and disposal	Dependence on intermediaries and manual intervention, limited transparency and traceability, data manipulation risks, and information delays.	Blockchain: tamper-resistant records, secure sharing, traceability, and smart contracts. IoT: real-time monitoring and lifecycle data collection.	Blockchain scalability, smart-contract execution time, gas consumption, transaction costs, reliable IoT integration, data security, and limited real-world validation.
[24] Liya et al. (2026)	Renewable Energy / Original Research	Secure and energy-efficient cyber-physical control of renewable microgrids using Edge-AI, IoT, and Blockchain	Limited integration of intelligent fault detection, secure energy transactions, and real-time decentralized control in renewable microgrids	Centralized control, conventional fault detection, and centralized energy authentication	Higher communication overhead, vulnerability to cyberattacks, limited real-time adaptability, and single-point-of-failure risks	SNN-based Edge-AI for cyber-fault detection and control optimization; Hyperledger Fabric for secure energy transactions, access control, and data provenance	Consensus latency, scalability, computational and energy overhead interoperability, and large-scale deployment challenges
[25] Ruihua Bai (2026)	Food supply chain logistics (cold-chain). Quantitative, simulation-based feasibility study using synthetic data.	Proactive contamination risk prediction, privacy-preserving cross-company collaboration, and immutable regulatory auditing.	Current blockchain systems lack predictive scoring; AI models lack regulatory alignment; data silos hinder collaboration; AI rarely integrates biological/physics knowledge.	Retrospective record-keeping, siloed databases, and reactive recalls after outbreaks occur.	Too slow to prevent harm, fragmented data, and commercial reluctance to share sensitive data centrally.	Blockchain: Secure ledgers for auditing data and models. AI: Advanced risk prediction and collaborative model training without sharing raw data	Reliance on synthetic data (lacks real-world validation); limited sensor inputs (needs CO ₂ /vibration); risk of model drift over time; need for stronger privacy safeguards (e.g., differential privacy).
[26] Rakesh Pal(2026)	Agriculture (smallholder farmers and Farmer Producer Organizations). Mixed-methods, multi-site quasi-experimental pilot study.	Improving price discovery, enabling faster automated payments, reducing post-harvest	Poor data quality at the collection edge, lack of platform interoperability, rural connectivity/digital literacy gaps, and undefined multi-party governance models.	Fragmented, multi-layered supply chains with heavy intermediation, manual quality checks, and delayed cash settlements.	Information asymmetry depresses farmgate prices, high rejection rates due to quality disputes, and lack of integrated access to formal finance.	Blockchain: Tokenizing produce lots, smart contracts for escrow/automated settlement, and immutable logistics notarization. AI: Price nowcasting, on-device quality grading (via smartphone images), and risk scoring for input credit/insurance.	Rural device/connectivity constraints, the "garbage in, garbage out" risk at data collection points, complex interoperability with legacy systems (e-NAM, banks), and strict data protection compliance (DPDP Act).
[27] Alamri, M., Tariq, N., Humayun, M., & Alshammeri, M. (2026)	Healthcare IoT (IoMT) and Edge/Fog Computing. Quantitative, simulation-based evaluation using benchmark datasets (BoT-IoT, ToN-IoT) with ablation and robustness testing.	Real-time, low-latency intrusion detection; tamper-evident auditing of security events; and energy-efficient threat classification at the network edge.	Centralized cloud models have high latency, fog systems lack auditability, traditional blockchains are too heavy for fog nodes, and IoT network traffic suffers from severe class imbalance.	Centralized cloud-based Intrusion Detection Systems (IDS); delayed log auditing; and heavy deep learning models (e.g., CNN, RNN) deployed centrally.	High transmission latency, single points of failure, inability to scale with massive IoT data volumes, and lack of transparent, tamper-proof logs for accountability.	Blockchain & AI Applications: Uses a lightweight, tamper-evident blockchain for secure edge logging and an optimized XGBoost AI model with SMOTE for rapid threat detection.	Relies on simulations (lacks live hardware testing), is vulnerable to data drift and adversarial attacks, faces edge-device storage limits for blockchain ledgers, and suffers from inflated performance metrics due to dataset biases.
[28] Khan, A. W., et al. (2026)	Cloud Computing Cybersecurity / Intrusion Detection Systems (IDS). Quantitative, experimental evaluation using the CICIDS2017 dataset and a simulated Ethereum (Ganache) network.	Real-time intelligent threat detection, decentralized user authentication, automated access control, and immutable forensic audit logging.	Blockchain-only systems lack intelligent threat detection; AI-only IDS lack tamper-proof logging and decentralized trust; existing integrated frameworks suffer from high computational overhead and poor scalability.	Centralized security architectures, basic firewalls, rule-based access control, and standalone machine learning models (e.g., SVM, Random Forest).	Single points of failure, vulnerability to log manipulation/insider threats, inability to detect complex temporal/zero-day attacks, and high false positive rates.	Blockchain: Decentralized SHA-256 authentication, immutable event logging, and Solidity smart contracts for automated policy enforcement. AI: Hybrid CNN-LSTM deep learning model for real-time intrusion detection (combining spatial feature extraction and temporal sequence learning), optimized with SMOTE for class imbalance.	Reliance on simulated local blockchain environments (lacks live production cloud validation); potential latency and gas cost bottlenecks in real-world deployments; need for future integration of federated learning, edge computing, and Explainable AI (XAI).

References	Sector / Study Type	Usage	Gaps	Traditional Mitigation Methods	Notable Weaknesses in Traditional Methods	Prominent Applications of Blockchain and AI	Research and Dissemination Challenges
[29] Gafsi, Hamdouni & Smaoui (2026)	Macro-level Sustainable Development (G20 panel econometrics)	Examines how FinTech adoption, AI readiness, and Blockchain activity jointly affect SDG performance across G20 economies (2015–2023) using CS-ARDL, AMG, CCEMG, and System GMM	Prior work studies FinTech, AI, and Blockchain in isolation rather than as complementary systems; macro-level (cross-country) evidence is scarce compared to firm/sector-level studies; narrow sustainability proxies (CO ₂ , ESG) used instead of a holistic SDG index; limited integration of Innovation-Driven Growth, TOE, and Institutional theories	Reliance on single-technology policy interventions (e.g., financial inclusion programs, R&D subsidies) treated as independent levers for sustainability	Fragmented, siloed digital policies capture only a fraction of potential sustainability gains; fail to account for cross-sectional dependence and slope heterogeneity across countries	AI-driven resource optimization, predictive environmental management, and ESG monitoring; FinTech-enabled financial inclusion and green finance; Blockchain-based ESG disclosure, carbon tracking, and transparent supply chains; strong FIN×AI, FIN×BLK, and AI×BLK complementarities	Composite indices (SDG Index) mask heterogeneity across individual goals; proxies (GitHub activity, Google Trends) imperfectly capture true blockchain adoption; short panel window (2015–2023) limits long-run inference; omitted institutional/governance variables risk bias
[30] Adebisi et al. (2026),	Cross-Border Finance / AML-Compliance (applied quantitative framework)	Proposes and simulates a Blockchain–AI Trust and Transparency Framework (B-AITTF) for cross-border payments, using panel regression, logistic regression on the Elliptic AML dataset, SEM, and Monte Carlo simulation	Few end-to-end, cross-border architectures integrate trust, transparency, and compliance; most studies are domestic/proof-of-concept only; governance mechanisms for enduring multi-jurisdictional accountability are under-addressed	Correspondent banking chains with sequential, institution-by-institution due diligence; rule-based AML/KYC monitoring; manual compliance checks	High intermediary depth and compliance steps sharply raise transaction costs; redundant, non-standardized verification creates opacity and delay; fragmented record-keeping weakens auditability and cross-jurisdictional data sharing	AI-based logistic/ML models for illicit-transaction detection (fraud detection accuracy 90.1%); blockchain as tamper-evident data substrate for KYC/AML records; smart contracts embedding compliance rules; combined framework cut simulated settlement time by over one-third	Regulatory fragmentation and divergent KYC/AML standards across jurisdictions limit model portability; AI models remain “black boxes,” complicating regulatory interpretability; blockchain immutability conflicts with data-protection/correction requirements; validator/infrastructure concentration undermines claimed decentralization
[31] Mishra & Mishra (2026)	FinTech Cybersecurity / Fraud Detection (systems architecture + simulation)	Develops an Adaptive Neuro-Fuzzy Blockchain–AI framework combining permissioned blockchain (PoA consensus) with ML and ANFIS-based risk inference for real-time fraud detection, tested on a 5-node consortium under normal/moderate/high-fraud scenarios	Existing hybrid frameworks emphasize either integrity (blockchain) or prediction (AI), rarely both jointly; blockchain evidence is typically used only for storage, not to actively modify AI risk decisions; limited explainability and adaptive learning in combined systems	Rule-based fraud detection systems; standalone supervised ML classifiers (Random Forest, SVM, XGBoost); centralized deep-learning models (LSTM, autoencoders); post-hoc blockchain verification	Rule-based systems can't scale to transaction volume/complexity, causing high false positives; centralized ML/DL risks privacy breaches and single points of failure; blockchain-only systems verify integrity but can't detect behavioral fraud; federated learning approaches lack dynamic, adaptive risk assessment	Dual-risk fusion of ML fraud probability and neuro-fuzzy inference; blockchain integrity indicators (hash validity, signature validity, validator approval, smart-contract compliance) directly modifying risk scores; tri-level Accept/Monitor/Reject decision model enforced via smart contracts; outperformed baseline hybrid models on accuracy, precision, and latency	Five-node consortium is a controlled proof-of-concept, not evidence of production-scale performance; cross-study comparisons with literature baselines are contextual only (different datasets/protocols, no direct statistical test); fixed fusion parameter (λ) not yet adaptively optimized; scalability under larger validator networks and real institutional data remains untested
[32] Shinde et al. (2026)	Healthcare — AI-based medical imaging security (brain tumor MRI diagnostics)	Protects MRI datasets for brain-tumor detection models from tampering. Raw scans are stored on a private IPFS network, while their cryptographic hashes are recorded on a Hyperledger Fabric ledger, allowing verification of who accessed an image and when.	Most prior defenses hardened the AI model itself (adversarial training, sanitization) rather than the dataset feeding it, leaving no way to prove an MRI scan was untouched before it ever reached the training pipeline.	Adversarial training; input sanitization (JPEG compression, denoising, autoencoders); digital watermarking and fingerprinting; trusted execution environments such as Intel SGX.	Computationally expensive and prone to overfitting on known attack types; sanitization can be bypassed by subtler perturbations; watermarking alters the original image and only detects tampering after the fact; TEEs need specialized hardware and can't verify a dataset's integrity before training even begins.	A Hyperledger Fabric permissioned network paired with private IPFS gives every MRI scan a content-addressed hash (CID) the instant it's uploaded, so even a single altered pixel is detectable. Role-based smart contracts (chaincode) govern uploads, access requests, and approvals, creating a fully auditable chain of custody from the diagnostic center onward.	Not yet linked to real hospital infrastructure (EMR/PACS); full HIPAA/GDPR compliance depends on organizational and legal measures beyond the technical layer; blockchain consensus and ledger upkeep add overhead that would need further tuning before deployment across many healthcare institutions.

References	Sector / Study Type	Usage	Gaps	Traditional Mitigation Methods	Notable Weaknesses in Traditional Methods	Prominent Applications of Blockchain and AI	Research and Dissemination Challenges
[33] Stephen et al. (2026)	Industrial waste management - coal gangue recycling and circular economy	Combines ResNet-50 image recognition, IoT sensors, and a Hyperledger Fabric blockchain to sort coal gangue by quality, monitor operations in real time, and log every transaction, letting emissions and recycling data be verified across 142 coal-processing sites.	Earlier work tackled AI-based sorting, IoT monitoring, or blockchain traceability separately; almost no study combined all three into one validated industrial system, and workforce displacement from automation was rarely addressed alongside the technology.	Manual sorting by workers; mechanical separation equipment (crushers, screens, density separators) based on the gangue's physical properties.	Manual sorting is slow, labor-intensive, and only about 68% accurate; mechanical separation is faster but still limited in precision, energy-hungry (roughly 40 kWh per ton), water-intensive, and costly to install and run.	A ResNet-50 model classifies gangue quality from camera images at the edge (Jetson TX2), IoT sensors stream data over LoRaWAN/5G, and a Hyperledger Fabric ledger timestamps every process step — pushing sorting accuracy to 95%, cutting energy use by 34%, and producing a tamper-proof record of carbon and recycling metrics.	Validation is limited to Shanxi and Inner Mongolia, which may affect generalizability to other coal types or regions; high throughput could lead to blockchain transaction latency issues, and economic viability is sensitive to capital costs and fluctuating energy prices, particularly for smaller plants.

3. Background: Complementary Properties

Blockchain facilitates decentralization, immutability, and governance through smart contracts, enabling interactions between untrusting parties without the need for middlemen [34]. Artificial Intelligence enhances pattern recognition, forecasting, and decision-making by analyzing large volumes of data and performing extensive computations. The two fields intersect in two significant ways: AI enhances distributed ledger technology within Blockchain, while Blockchain supplies secure and trustworthy data for AI models [35][36]. The figure below shows the structure for integrating the two technologies, highlighting key applications, challenges, and future directions.

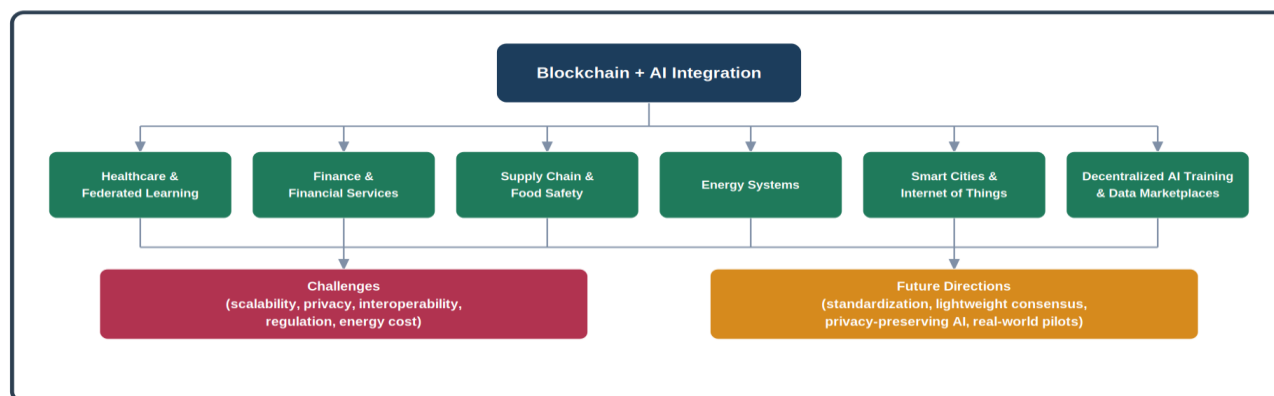


Figure 1. Blockchain–AI Integration: Applications, Challenges, and Future Directions

4. Applications

4.1 Healthcare and Federated Learning

Healthcare is the most active area in the literature because federated learning enables hospitals to train diagnostic models collaboratively without relocating patient data. At the same time, blockchain provides an auditable record of model updates and contributions [37]. Recent surveys identify three main technical patterns for integrating federated learning with distributed ledgers in smart healthcare systems: blockchain-enabled model storage, aggregation, and gradient upload [38]. This work integrates homomorphic encryption with blockchain-based federated learning to protect privacy and mitigate risks from centralized aggregators, aiming to comply with regulations like GDPR and HIPAA while promoting inter-institutional collaboration [39].

4.2 Finance and Financial Services

Blockchain technology enhances information transparency and authenticity in the finance industry, while artificial intelligence technology enables fraud detection to be more accurate and enhances credit scores [40]. The combination of both technologies in the financial industry increases the security and efficiency of financial processes. Blockchain technology guarantees the security of transactions, whereas AI analyses the data for anomalies [41].

4.3 Supply Chain and Food Safety

Combining blockchain technology with anomaly detection capabilities of AI in supply chains offers tamper-proof traceability of the former along with risk evaluation by the latter through sensor data [42]. Blockchain use in food safety requires monitoring its origin and handling processes, while artificial intelligence uses IoT sensor data to monitor contamination risks [43].

4.4 Energy Systems

Combining blockchain and artificial intelligence is transforming energy management by decentralized market systems, grid management, and improved decision-making [44]. Blockchain technology creates an environment for secure peer-to-peer transactions and automated processes via smart contracts, while AI helps predict energy needs and identify anomalies within the grid [45][46].

4.5 Smart Cities and the Internet of Things

A smart city shows the importance of integrating Blockchain technology, AI, and the Internet of Things (IoT) to deliver sustainable and secure urban services [47]. Although IoT devices generate data from various systems, large-scale deployment leads to problems with authentication, security, privacy, and trust [48]. On the other hand, AI can help analyze the generated data to make informed decisions. Blockchain can provide an infrastructure to ensure secure data and transaction handling [49]. The combination of AI and blockchain can benefit smart energy applications within smart cities [50].

4.6 Decentralized AI Training and Data Marketplaces

The latest research focuses on the role of blockchain technology in developing decentralized AI systems, where token incentives and proof of contributions through the blockchain can help improve collaboration and increase trust [51]. Blockchain technology makes it possible to train the AI system in a decentralized manner by making it possible for parties to share their local data and computing capabilities by exchanging model parameters [52].

5. Challenges

Nevertheless, scaling and latency problems remain, mainly due to inefficiency of consensus algorithms that affects transaction throughput. Application of AI-based solutions, especially reinforcement learning for proof-of-stake optimization, can improve consensus latency by 30-50%, but such solutions have drawbacks concerning energy consumption and training expenses [50]. Computational and energy cost is a second constraint, since running AI training or inference on-chain, or verifying it through consensus, can be substantially more expensive than equivalent off-chain computation due to computational overhead and transaction costs[53]. The oracle problem needs to be handled through sourcing of data from multiple independent sources and their validation before recording the same on the blockchain. Source validation, cross-source consistency check, and anomaly detection can help in identifying any potentially fraudulent or unreliable data [54], [55]. In case of federated learning, client model updates need to be evaluated and checked before adding the same to the blockchain using consistency and anomaly-detection techniques to identify the presence of any potentially malicious data [56], [57]. The suspicious data can be denied while the validated data can be sent to be verified using the blockchain technology. Artificial intelligence-based vulnerability analysis can aid in analyzing the potential security vulnerabilities present in blockchain-related applications and smart contracts [58], [59]. After passing through all the necessary validation processes, the blockchain validators can use the underlying consensus algorithm before committing the same to the blockchain. Nevertheless, the process of blockchain consensus just guarantees agreement on the legitimacy of the presented data based on the consensus protocol, but it cannot ensure semantic accuracy of the underlying data [60]. The approach of privacy-preserving federated learning could further help to minimize the amount of exposure of sensitive data in the process of collaborative modeling. The application of AI in the identification of anomalies and attacks may serve as an additional component [61]. When using systems with heterogeneous data sources, the issue of cross-platform integration becomes relevant and requires data transfer and interoperability solutions to be implemented [62], [63]. Layer-2 proving schemes and other methods of verification may be used in cases of moving computational processes from the main blockchain [64].

6. Future Directions

A number of important themes have emerged from the review of literature. First, it is very likely that lightweight and layer-2 designs where AI processing is moved away from the base blockchain, while proofs or hashes are kept on chain, will continue to prevail as an effective solution of matching computing requirements of AI with throughput capacity of blockchain technology [65][66]. Second, the federated and decentralized training marketplace using blockchain technology solely for incentive and provenance purposes, but not for computations themselves, provides a viable middle ground between centralized and on-chain training of AI [67]. Third, AI-aided validation of smart contracts is expected to be adopted because of the observed reduction in vulnerabilities. Nonetheless, the protection of the auditing model from adversarial manipulation remains an unresolved challenge [68]. Fourth, the integration of explainable AI with blockchain is a promising approach to enhance algorithmic transparency and accountability, especially in sensitive areas like healthcare. Blockchain offers tamper-resistant records of model updates, while XAI enhances the interpretability of AI decisions [69]. Finally, interoperability and standardization of blockchain networks are important in moving blockchain-AI systems from standalone projects to infrastructure. Lack of standards can lead to fragmentation, lack of scalability, and inefficient data management [70].

7. Conclusion

The integration between blockchain and artificial intelligence is no longer a mere academic concept, but it is an existing field of research where real results have been obtained in fields like health care, finance, logistics, energy, smart cities, and decentralized AI. The common denominator between all these applications is the combination between blockchain which provides verifiable trust and coordination and AI which provides intelligent adaptiveness, and in the successful cases, the appropriate task to be performed by each technology is determined. The principal barriers, scalability, cost, data quality, interoperability, privacy, and regulation, are technical as much as institutional, and progress will likely depend on continued work at their intersection rather than on either technology in isolation.

References

- [1] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2019. <https://doi.org/10.1016/j.rser.2018.10.014>
- [2] S. Makridakis and K. Christodoulou, "Blockchain: Current challenges and future prospects/applications," *Future Internet*, vol. 11, no. 12, p. 258, 2019, doi: 10.3390/fi11120258.
- [3] Z. Ngoupayou Limbepe, K. Gai, and J. Yu, "Blockchain-based privacy-enhancing federated learning in smart healthcare: A survey," *Blockchains*, vol. 3, no. 1, p. 1, 2025, doi: 10.3390/blockchains3010001.
- [4] G. Tripathi, M. A. Ahad, and G. Casalino, "A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges," *Decision Analytics Journal*, vol. 9, p. 100344, 2023, doi: 10.1016/j.dajour.2023.100344.
- [5] J. Shi and Y. Wang, "Academic exploration of blockchain and AI in financial services," *Journal of Electronic Business & Digital Economics*, vol. 4, no. 2, pp. 270–282, 2025, doi: 10.1108/JEBDE-08-2024-0023.
- [6] T. Handra, N. Lutfiani, A. Aprillia, F. P. Oganda, F. Amelia, and N. Rangi, "Adaptive workflow management with decentralized AI in blockchain based distributed ledger systems," *Blockchain Frontier Technology*, vol. 5, no. 1, pp. 71–79, 2025, doi: 10.34306/bfront.v5i1.804.
- [7] B. Shrimali and H. B. Patel, "Blockchain state-of-the-art: Architecture, use cases, consensus, challenges and opportunities," *Journal of King Saud University – Computer and Information Sciences*, vol. 34, no. 9, pp. 6793–6807, 2022, doi: 10.1016/j.jksuci.2021.08.005.
- [8] I. Shah, W. Dange, N. Nirgule, and D. Ilme, "Next-generation digital voting system," *International Journal of Computational and Electronic Aspects in Engineering*, vol. 2, no. 3, pp. 71–75, Jul. 2021, doi: 10.26706/ijceae.2.3.20210606.
- [9] A. Alhaidari, B. Palanisamy, and P. Krishnamurthy, "On-Chain Decentralized Learning and Cost-Effective Inference for DeFi Attack Mitigation," in *Proc. 7th Conference on Advances in Financial Technologies (AFT 2025)*, LIPIcs, vol. 354, pp. 35:1–35:27, 2025, doi: 10.4230/LIPIcs.AFT.2025.35.

- [10] R. Lavin, X. Liu, H. Mohanty, L. Norman, G. Zaarour, and B. Krishnamachari, "A survey on the applications of zero-knowledge proofs," arXiv preprint arXiv:2408.00243, 2024, doi: 10.48550/arXiv.2408.00243.
- [11] L. T. Thibault, T. Sarry, and A. S. H. Hafid, "Blockchain scaling using rollups: A comprehensive survey," *IEEE Access*, vol. 10, pp. 123775–123813, 2022, doi: 10.1109/ACCESS.2022.3200051.
- [12] N. Köhl, M. Schemmer, M. Goutier, and G. Satzger, "Artificial intelligence and machine learning," *Electronic Markets*, vol. 32, no. 4, pp. 2235–2244, 2022, doi: 10.1007/s12525-022-00598-0.
- [13] J. Zhang, Y. Che, R. Liu, Z. Wang, and W. Liu, "Deep learning-driven multi-omics analysis: Enhancing cancer diagnostics and therapeutics," *Briefings in Bioinformatics*, vol. 26, no. 4, p. bbaf440, 2025, doi: 10.1093/bib/bbaf440.
- [14] S. Ahmed, M. S. Kaiser, S. Chaki, S. Aloteibi, and M. A. Moni, "Federated learning model with dynamic scoring-based client selection for diabetes diagnosis," *Knowledge-Based Systems*, vol. 320, Art. no. 113662, 2025, doi: 10.1016/j.knsys.2025.113662.
- [15] D. Bhumichai, C. Smiliotopoulos, R. Benton, G. Kambourakis, and D. Damopoulos, "The convergence of artificial intelligence and blockchain: The state of play and the road ahead," *Information*, vol. 15, no. 5, p. 268, 2024, doi: 10.3390/info15050268.
- [16] M. M. Orabi, O. Emam, and H. Fahmy, "Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: Literature review," *Journal of Big Data*, vol. 12, p. 55, 2025, doi: 10.1186/s40537-025-01099-5.
- [17] Y. Zuo, "Exploring the synergy: AI enhancing blockchain, blockchain empowering AI, and their convergence across IoT applications and beyond," *IEEE Internet of Things Journal*, vol. 12, no. 6, pp. 6171–6195, 2025, doi: 10.1109/JIOT.2024.3507746.
- [18] O. Kuznetsov, P. Sernani, L. Romeo, E. Frontoni, and A. Mancini, "On the integration of artificial intelligence and blockchain technology: A perspective about security," *IEEE Access*, vol. 12, pp. 3881–3897, 2024, doi: 10.1109/ACCESS.2023.3349019.
- [19] R. K. Veerapaneni and R. Delhibabu, "Trustworthy intelligent rooms: Integrating blockchain, federated learning, and data-centric AI for healthcare 4.0," *Frontiers in Digital Health*, vol. 8, art. 1758304, 2026, doi: 10.3389/fdgth.2026.1758304.
- [20] S. Bulut, "Artificial intelligence research in smart cities: A bibliometric analysis," *Kent Akademisi*, vol. 19, no. 2, pp. 1–22, 2026, doi: 10.35674/kent.1669862.
- [21] N. Arshadi and T. P. Dombrowski, "Applications and management of blockchain technologies in financial services," *Journal of Risk and Financial Management*, vol. 19, no. 3, p. 224, 2026, doi: 10.3390/jrfm19030224.
- [22] M. Iqbal, Z. Zahraani, H. Ilmi, M. Mutasar, P. Naila, and E. Marra, "Mitigating religious radicalism and polarization through the integration of artificial intelligence (AI), internet of things (IoT), blockchain and cognitive science," *AMPLITUDE: Journal of Science and Technology Innovation*, vol. 5, no. 1, pp. 148–157, 2026, doi: 10.56566/amplitulo.v5i1.551.
- [23] D. Upadhyay, P. Garg, and N. Babbar, "Blockchain and IoT based smart contract framework for efficient and secure product life management," *Discover Internet of Things*, vol. 6, p. 25, 2026, doi: 10.1007/s43926-025-00274-7.
- [24] B. S. Liya, H. Kumar, M. M. M. Hassan, P. Nisha, M. G. Aush, and D. Anand, "Energy efficient cyber-physical control of renewable microgrids using edge-AI enabled IoT and secure blockchain coordination," *Scientific Reports*, vol. 16, art. 20194, 2026, doi: 10.1038/s41598-026-50169-y.
- [25] R. Bai, "Integration of blockchain and AI knowledge management for contamination risk prediction in food logistics," *Engineering Reports*, vol. 8, art. e70944, 2026, doi: 10.1002/eng2.70944.
- [26] R. Pal, "Decentralized market access for farmers using blockchain-AI tools," *Scientific Journal of Artificial Intelligence and Blockchain Technologies*, vol. 3, no. 3, pp. 17–24, Jul.–Sep. 2026.
- [27] M. Alamri, N. Tariq, M. Humayun, and M. Alshammeri, "Energy-efficient threat detection in IoT healthcare using AI and blockchain-enhanced fog-cloud architecture," *Cluster Computing*, vol. 29, Art. no. 108, 2026, doi: 10.1007/s10586-025-05932-7.
- [28] A. W. Khan, A. Muhammad, Farhan, A. Salam, A. K. K. Baig, M. Tahir, and N. H. Ansari, "An AI-driven blockchain-based cybersecurity framework for secure cloud computing environments," *Spectrum of Engineering Sciences*, vol. 4, no. 6, pp. 1745–1762, 2026, doi: 10.5281/zenodo.20728226.

- [29] N. Gafsi, A. Hamdouni, and A. Smaoui, "Digital technologies and sustainable development: Evidence from FinTech, AI, and blockchain adoption in G20 economies," *Sustainability*, vol. 18, no. 5, art. 2484, 2026, doi: 10.3390/su18052484.
- [30] O. O. Adebisi, A. D. Popoola, P. D. Adeyinka, A. T. Arigbabu, and O. O. Olateju, "Blockchain-integrated AI systems for enhancing trust and transparency in cross-border finance," *Asian Journal of Research in Computer Science*, vol. 19, no. 1, pp. 271–291, 2026, Art. no. AJRCOS.151919, doi: 10.9734/ajrcos/2026/v19i1818.
- [31] G. Mishra and Y. Mishra, "An adaptive neuro-fuzzy blockchain–AI framework for secure and intelligent FinTech transactions," *Scientific Reports*, 2026, Art. in press, doi: 10.1038/s41598-026-66643-6.
- [32] R. Shinde, S. Patil, K. Kotecha, and S. Mishra, "Ensuring the integrity of AI models: A blockchain-based approach for protecting medical imaging training data," *Scientific Reports*, vol. 16, no. 1, art. 13989, 2026, doi: 10.1038/s41598-026-44040-3.
- [33] A. O. Stephen, C. Liu, and G. Xin, "A smart AI–IoT–blockchain framework for sustainable coal gangue waste systems and circular resource recovery," *Cleaner Waste Systems*, vol. 14, Art. no. 100497, 2026, doi: 10.1016/j.clwas.2026.100497.
- [34] J. Singh, S. Bharany, S. Rani, A. U. Rehman, B. M. Taye, and R. Pant, "A systematic review of blockchain, AI, and cloud integration for secure digital ecosystems," *International Journal of Networked and Distributed Computing*, vol. 13, p. 28, 2025, doi: 10.1007/s44227-025-00072-1.
- [35] A. I. Kathia, P. Tasca, Y. Erinle, N. Vadgama, A. Satybaldy, and M. A. Javarone, "SoK: A systematic bidirectional literature review of AI & DLT convergence," arXiv preprint arXiv:2605.10515, 2026, doi: 10.48550/arXiv.2605.10515.
- [36] K. D. Pandl, S. Thiebes, M. Schmidt-Kraepelin, and A. Sunyaev, "On the convergence of artificial intelligence and distributed ledger technology: A scoping review and future research agenda," *IEEE Access*, vol. 8, pp. 57075–57095, 2020, doi: 10.1109/ACCESS.2020.2981447.
- [37] T. Bhardwaj and K. Sumangali, "An explainable federated blockchain framework with privacy-preserving AI optimization for securing healthcare data," *Scientific Reports*, vol. 15, art. 21799, 2025, doi: 10.1038/s41598-025-04083-4.
- [38] R. Shinde, S. Patil, K. Kotecha, V. Potdar, G. Selvachandran, and A. Abraham, "Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions," *Engineering Technology & Engineering*, 2023, doi: 10.1002/ett.4884.
- [39] V. Punniyamoorthy, A. G. Parthi, M. Palanigounder, R. K. Kodali, B. Kumar, and K. Kannan, "A privacy-preserving cloud architecture for distributed machine learning at scale," arXiv preprint arXiv:2512.10341, 2025.
- [40] A. M. Al Shareef, S. Seçkiner, B. Eid, and H. Abumeteir, "Integration of blockchain with artificial intelligence technologies in the energy sector: A systematic review," *Frontiers in Energy Research*, vol. 12, art. 1377950, 2024, doi: 10.3389/fenrg.2024.1377950.
- [41] "Augmented finance for climate action: A systematic review of AI, IoT, and blockchain applications in sustainable finance," *International Journal of Financial Studies*, vol. 14, no. 4, art. 91, 2026, doi: 10.3390/ijfs14040091.
- [42] M. R. Sebti, U. McCarthy, A. Ktenioudaki, M. Russo, and M. Merenda, "Traceability and anti-counterfeiting in agri-food supply chains: A review of RFID, IoT, blockchain, and AI technologies," *Sensors*, vol. 26, no. 5, art. 1685, 2026, doi: 10.3390/s26051685.
- [43] S. B. Dhal and D. Kar, "Leveraging artificial intelligence and advanced food processing techniques for enhanced food safety, quality, and security: A comprehensive review," *Discover Applied Sciences*, vol. 7, no. 1, art. 75, 2025, doi: 10.1007/s42452-025-06472-w.
- [44] O. O. Egunjobi, A. Gomes, C. N. Ekwim, and H. Morais, "A systematic review of blockchain for energy applications," *e-Prime – Advances in Electrical Engineering, Electronics and Energy*, vol. 9, art. 100751, 2024, doi: 10.1016/j.prime.2024.100751.
- [45] H. Majidi, M. M. Hayati, C. Breyer, B. Mohammadi-ivatloo, S. Honkapuro, H. Karjunen, P. Laaksonen, and V. Sihvonen, "Overview of energy modeling requirements and tools for future smart energy systems," *Renewable and Sustainable Energy Reviews*, vol. 212, art. 115367, 2025, doi: 10.1016/j.rser.2025.115367.

- [46] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
- [47] I. Lukić et al., "Advancing smart city sustainability through artificial intelligence, digital twin and blockchain solutions," *Technologies*, vol. 13, no. 7, art. 300, 2025, doi: 10.3390/technologies13070300.
- [48] A. Alotaibi, H. Aldawghan, and A. Aljughaiman, "A review of the authentication techniques for internet of things devices in smart cities: Opportunities, challenges, and future directions," *Sensors*, vol. 25, no. 6, art. 1649, 2025, doi: 10.3390/s25061649.
- [49] A. Denis, A. Thomas, W. Robert, A. Samuel, S. P. Kabiito, Z. Morish, M. Sallam, G. Ali, and M. M. Mijwil, "A survey on artificial intelligence and blockchain applications in cybersecurity for smart cities," *SHIFRA*, vol. 2025, pp. 1–45, 2025, doi: 10.70470/SHIFRA/2025/001.
- [50] Y. Y. Ghadi, T. Mazhar, T. Shahzad, I. H. Jaghdam, S. Khan, M. A. Khan, and H. Hamam, "A hybrid AI-Blockchain security framework for smart grids," *Scientific Reports*, vol. 15, no. 1, art. 20882, 2025, doi: 10.1038/s41598-025-05257-w.
- [51] A. M. Shamsan Saleh, "Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review," *Blockchain: Research and Applications*, 2024, doi: 10.1016/j.bcra.2024.100193.
- [52] X. Hui and C. E. Tucker, "Decentralization, blockchain, artificial intelligence (AI): Challenges and opportunities," *Journal of Product Innovation Management*, vol. 42, no. 5, pp. 947–957, 2025, doi: 10.1111/jpim.12800.
- [53] G. Mandinyanya and V. Malele, "Synthesizing the future of AI-blockchain integration: A pathway for adaptive, ethical, and efficiency," *Latin-American Journal of Computing*, vol. 13, no. 1, pp. 23–33, 2026, doi: 10.33333/lajc.vol13n1.02.
- [54] G. Caldarelli, "Can artificial intelligence solve the blockchain oracle problem? Unpacking the challenges and possibilities," *Frontiers in Blockchain*, vol. 8, art. 1682623, 2025, doi: 10.3389/fbloc.2025.1682623.
- [55] M. F. Mahdi, "Enhancing cloud security through artificial intelligence: Detecting advanced cyber attacks and analyzing anomalous patterns," *International Journal of Computational and Electronic Aspects in Engineering*, vol. 6, no. 3, pp. 108–120, Jun. 2025, doi: 10.26706/ijceae.6.3.20250601.
- [56] Y. M. Abdal, "AI-driven privacy shield: A secure and privacy-preserving federated learning framework," *International Journal of Computational and Electronic Aspects in Engineering*, vol. 6, no. 3, pp. 180–189, Jul. 2025, doi: 10.26706/ijceae.6.3.20250608.
- [57] X. Gu, F. Sabrina, Z. Fan, and S. Sohail, "A review of privacy enhancement methods for federated learning in healthcare systems," *International Journal of Environmental Research and Public Health*, vol. 20, no. 15, art. 6539, 2023, doi: 10.3390/ijerph20156539.
- [58] M. Q. Mohammed and Z. A. Jaaz, "A comprehensive review of predictive vulnerability prioritization using AI," *International Journal of Computational and Electronics Aspects in Engineering*, vol. 7, no. 1, pp. 27–44, Feb. 2026, doi: 10.26706/ijceae.7.1.20260103.
- [59] M. Ozdag, "AI-driven vulnerability analysis in smart contracts: Trends, challenges and future directions," *International Journal of Artificial Intelligence and Applications (IJAI)*, vol. 16, no. 3, pp. 65–82, May 2025, doi: 10.5121/ijaia.2025.16305.
- [60] N. Choi and H. Kim, "Technological convergence of blockchain and artificial intelligence: A review and challenges," *Electronics*, vol. 14, no. 1, art. 84, 2024, doi: 10.3390/electronics14010084.
- [61] W. Ibrar, D. Mahmood, A. S. Al-Shamayleh, G. Ahmed, S. Z. Alharthi, and A. Akhunzada, "Generative AI: A double-edged sword in the cyber threat landscape," *Artificial Intelligence Review*, vol. 58, no. 9, art. 285, 2025, doi: 10.1007/s10462-025-11285-9.
- [62] H. Yuan, S. Fei, and Z. Yan, "Technologies of blockchain interoperability: A survey," *Digital Communications and Networks*, vol. 11, no. 1, pp. 210–224, 2025, doi: 10.1016/j.dcan.2023.07.008.
- [63] Y. A. Turkey, "Transferring heterogeneous database data to relational systems using HTTP and JSON," *International Journal of Computational and Electronic Aspects in Engineering*, vol. 7, no. 1, pp. 1–11, Feb. 2026, doi: 10.26706/ijceae.7.1.20260101.
- [64] D. Tortola, A. Lisi, P. Mori, and L. Ricci, "Tethering Layer 2 solutions to the blockchain: A survey on proving schemes," *Computer Communications*, vol. 225, pp. 289–310, 2024, doi: 10.1016/j.comcom.2024.07.017.

- [65] M. S. Al Jasem, T. De Clark, and A. K. Shrestha, "Toward decentralized intelligence: A systematic literature review of blockchain-enabled AI systems," *Information*, vol. 16, no. 9, art. 765, 2025, doi: 10.3390/info16090765.
- [66] E. Lui, R. Sun, V. Shah, X. Xiong, J. Sun, D. Crapis, W. Knottenbelt, and Z. Wang, "SoK: Blockchain-Based Decentralized AI (DeAI)," in *Proc. IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)*, 2026. doi: 10.48550/arXiv.2411.17461.
- [67] S. Alsunaidi, H. Aljamaan, and M. Hammoudeh, "Leveraging machine learning models to improve smart contract security: A survey of vulnerabilities and detection methods," *ACM Computing Surveys*, vol. 58, no. 6, art. 151, pp. 1–37, 2025, doi: 10.1145/3772367.
- [68] R. Asif, S. R. Hassan, and G. Parr, "Integrating a blockchain-based governance framework for responsible AI," *Future Internet*, vol. 15, no. 3, art. 97, 2023, doi: 10.3390/fi15030097.
- [69] D. Kaushik, P. Gulia, N. S. Gill, M. Yahya, P. K. Shukla, and J. Shreyas, "Synergizing blockchain and AI to fortify IoT security: A comprehensive review," *Artificial Intelligence Review*, vol. 59, art. 41, 2026, doi: 10.1007/s10462-025-11434-0.
- [70] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A Survey on Blockchain Interoperability: Past, Present, and Future Trends," *ACM Computing Surveys*, vol. 54, no. 8, Art. 168, 2022. doi: 10.1145/3471140.