International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Enhancing Lost Item Retrieval through AI-Powered Blockchain

Kankata Venkata Narayana *, Nallajarla Sai Gopal, Nirmal Pandey and Kadamati Aditya Venkata Sri Sai

Department of CSE, Aditya College of Engineering & Technology, Surampalem, Kakinada.

International Journal of Science and Research Archive, 2026, 18(02), 975-982

Publication history: Received on 16 January 2026; revised on 23 February 2026; accepted on 26 February 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.18.2.0360

Abstract

Traditional lost and found systems in institutions often rely on manual registers or centralized software, resulting in limited transparency, weak auditability, and frequent ownership conflicts. Such systems typically depend on manual comparison of item descriptions, which is time-consuming and prone to human error. Blockchain technology provides a decentralized and tamper-resistant mechanism for secure data storage and verification [1], [3]. This paper presents a Lost and Found Management System that integrates blockchain with an artificial intelligence-based matching module to enhance security and retrieval efficiency. Instead of storing complete records on-chain, the system stores cryptographic hashes while maintaining item data in secure off-chain storage to ensure scalability and data integrity [4], [5]. Smart contracts automate claim validation and reduce reliance on manual verification processes [8], [9]. Additionally, the AI model analyzes both textual descriptions and images to generate accurate match predictions, leveraging advancements in deep learning-based object detection [7]. Experimental evaluation using sample datasets demonstrates improved Blockchain matching consistency, enhanced record tracking, and greater reliability compared to traditional lost and found approaches.

Keywords: Blockchain: Artificial Intelligence:Lost and Found Management System: Smart Contracts: Deep Learning-Based Object Detection: Cryptographic Hashing

1. Introduction

The occurrence of misplaced or lost items has increased significantly with the growth of student populations and their daily movement within institutional environments. Traditional lost and found records are commonly managed through manual registers or centralized digital systems across colleges, offices, and public organizations. Although these methods are simple to maintain, they lack transparency and offer limited protection against data manipulation or false ownership claims. Furthermore, the absence of a reliable audit trail makes it difficult to track record modifications, thereby reducing overall system trust [2], [3].

Manual matching of lost and found items presents another major limitation in existing systems. Administrators typically compare descriptions or images manually, a process that is both time- consuming and prone to human error. Ownership conflicts often arise when multiple individuals claim the same item, and without a secure verification mechanism, resolving such disputes becomes challenging. These constraints reduce user confidence and increase administrative workload.

Blockchain technology offers a decentralized and tamper-resistant approach to data storage and verification through cryptographic hashing and distributed consensus mechanisms [1], [5].

* Corresponding author: Kankata Venkata Narayana

Once recorded on a blockchain ledger, data becomes immutable, ensuring that any unauthorized modification is easily detectable. In addition, smart contracts enable automated and transparent execution of predefined rules, eliminating reliance on centralized intermediaries [8], [9].

2. Literature Survey:

Lost and found management has traditionally relied on manual registers or centralized online platforms operated by institutions, transportation authorities, and public venues. While such systems provide basic record-keeping capabilities, they lack strong data integrity, traceability, and secure ownership transfer mechanisms. Centralized databases remain vulnerable to data manipulation and often fail to maintain transparent audit trails, thereby reducing confidence in dispute resolution processes [2], [3]. Moreover, manual verification and item matching become increasingly inefficient as the volume of reports grows, leading to delays and higher administrative workload.

Blockchain technology has gained significant research attention for applications such as supply chain monitoring, digital identity validation, and secure asset tracking due to its immutability and decentralized trust model [1], [30]. Smart contracts further enhance these systems by enabling automated, transparent, and rule-based transaction execution without relying on centralized intermediaries [8], [9]. However, most blockchain-based registries primarily focus on digital assets and financial transactions, with limited exploration of their potential for physical object recovery and real-world lost and found workflows.

In parallel, Artificial Intelligence (AI) techniques, particularly image recognition and similarity detection, have demonstrated strong performance in object identification and visual matching tasks. Deep learning models such as real-time object detection frameworks significantly improve feature extraction and classification accuracy [7], [24]. These AI-driven approaches reduce manual effort and enhance matching precision. Despite these advancements, few existing systems successfully integrate blockchain-based record integrity with AI-powered image matching, geo-location services, anonymous return mechanisms, and automated reward management within a unified architecture. The convergence of blockchain and AI has been increasingly recognized as a promising direction for building secure, intelligent, and scalable digital platforms [19], [22], [29]. This research gap highlights the need for a privacy-preserving and efficient registry designed specifically for managing physical lost and found items in real- world community environments.

3. Existing & Proposed System:

3.1. Existing System:

Lost and found management in real-world environments such as transportation centers, shopping malls, offices, and residential areas is commonly handled through manual registers or centralized digital platforms. These methods depend heavily on administrative personnel to document item details and validate ownership claims, but they often lack transparency in data updates and modifications. As a result, verifying whether records have been altered becomes challenging, and the absence of an immutable audit trail reduces overall system trust and accountability [2], [3]. Additionally, manual comparison of item descriptions or images is time- consuming and prone to human error, limiting the efficiency of the matching process. Research indicates that centralized architectures are vulnerable to data tampering and security risks, making them less suitable for sensitive record management [1], [30]. Privacy concerns further arise during claim verification due to the need for direct sharing of personal information, while reward mechanisms are typically informal and lack secure automation. These limitations highlight the need for decentralized and secure solutions capable of improving transparency, traceability, and operational efficiency[19],[22].

3.2. Proposed System:

The proposed system introduces a blockchain-based Lost and Found registry designed to improve the recovery of physical objects within institutional and community environments. Unlike traditional centralized databases, the system stores cryptographic hash values of item reports on a blockchain ledger, ensuring immutability, traceability, and enhanced data integrity [1], [5]. Actual item details, including images and descriptions, are securely maintained in off-chain storage to improve system scalability while preserving verifiable records through distributed file systems such as IPFS [4]. This hybrid architecture guarantees that once an item is registered, any unauthorized modification becomes immediately detectable, thereby increasing transparency and user trust.

Additionally, the system integrates Artificial Intelligence-based image and text matching techniques to automatically identify and rank potential matches, leveraging advancements in deep learning for object recognition [7], [24]. Smart

contracts are employed to automate claim validation and optional reward escrow processes, enabling secure and transparent transactions without reliance on intermediaries [8], [9]. The platform further incorporates geo-tagging to enhance location-based search efficiency and supports QR code-enabled anonymous returns to protect user privacy. By combining blockchain, AI, and decentralized technologies, the proposed solution delivers a secure, privacy-preserving, and scalable framework for modern lost and found management [19], [29].

4. Methodology

The proposed architecture, illustrated in Figure 1, presents a secure and privacy-preserving lost and found management system that integrates blockchain technology, encrypted off-chain storage, artificial intelligence-based item matching, and smart contract automation. Users report lost or found items through a secure web or mobile interface by providing details such as item description, images, geo-location tags, and optional reward information. Submitted data undergo preprocessing, where images are transformed into feature representations for similarity analysis and textual descriptions are structured using natural language processing techniques.

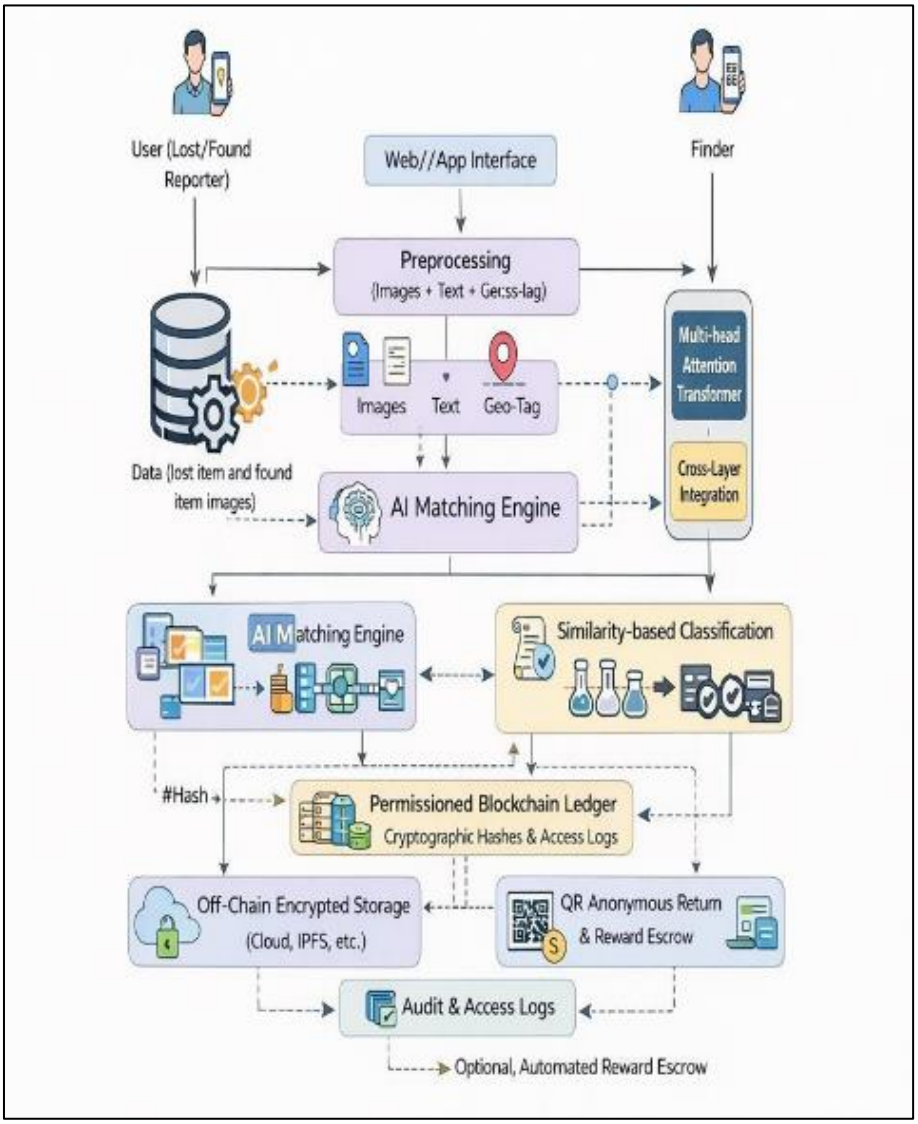

Figure 1 Architecture of the Proposed AI-Powered Blockchain-Based Lost and Found Management System

To ensure data integrity, each item record is converted into a unique cryptographic hash using SHA-256 before being recorded on a permissioned blockchain ledger, enabling tamper-resistant and verifiable storage [5], [1]. Instead of storing complete records on-chain, only hashes and essential metadata are maintained, while images and related data are securely stored in encrypted off-chain repositories such as cloud platforms or IPFS to enhance scalability and efficiency [4], [27].

A smart contract layer enforces role-based access control and automates claim management, allowing users to submit ownership requests that are validated through predefined logic while optional reward escrow is handled transparently on the blockchain [8], [9]. Additionally, QR code-enabled anonymous reporting supports privacy-preserving item returns without requiring direct disclosure of personal information. The AI-powered matching engine continuously evaluates image similarity, textual relevance, and geo-spatial proximity to rank potential matches, leveraging advancements in deep learning-based object recognition [7], [24]. By combining decentralized storage, intelligent automation, and secure verification mechanisms, the overall architecture ensures tamper resistance, privacy protection, automated governance, and an efficient recovery workflow suitable for modern digital ecosystems [19], [30].

5. Experiments and Results

5.1. Data Collection.

To evaluate the proposed system, a synthesized dataset of lost and found records was developed to replicate real-world reporting scenarios across public and community environments. The dataset included commonly misplaced items such as mobile phones, wallets, ID cards, bags, and electronic devices, with each entry containing text descriptions, images, and geo-location metadata. Artificial variations in lighting, image angles, and description styles were introduced to improve system robustness. Deep learning-based feature extraction techniques were utilized to enhance recognition accuracy [7], while blockchain integration ensured secure and tamper-resistant record verification throughout the evaluation [1], [30].

5.2. Preprocessing and Hash Generation.

All uploaded item records underwent preprocessing, where textual data was normalized and tokenized to enable similarity detection, while images were resized and converted into feature embeddings using convolutional neural networks for improved recognition accuracy [7]. After preprocessing, each record was assigned a unique SHA-256 cryptographic hash and stored on a permissioned blockchain as a reference identifier, ensuring data immutability and integrity [5], [1]. The detailed item information was securely maintained in encrypted off-chain storage to enhance scalability and protect sensitive data [4]. Any unauthorized modification results in a hash mismatch, allowing immediate detection of data tampering and strengthening overall system trust [3].

5.3. Blockchain Statemetn of Integrity.

Smart contracts compatible with Ethereum were deployed within a permissioned blockchain environment to ensure secure and verifiable record management [9], [1]. Each uploaded item generated a unique ledger entry in the form of a cryptographic hash, enabling immutable storage. During claim validation or data retrieval, the system recomputed the hash and compared it with the on-chain value to detect any unauthorized modifications. This hash-based verification mechanism ensures data integrity, prevents tampering, and strengthens trust in the authenticity of records [5], [3].

5.4. Smart (Claim and Reward Management) based on Smart Contracts.

Claim requests, approvals, and optional reward escrow were managed through role-based smart contracts to ensure secure and automated transaction handling [8], [9]. Once the AI engine identified a potential match, the claimant could initiate a request that triggered predefined smart contract validation logic. Any associated reward was temporarily held in escrow until ownership confirmation was completed, ensuring fairness and transparency. All transactions, including approvals and payments, were permanently recorded on the blockchain to provide auditability, eliminate human bias, and enhance trust in the system [1], [3].

5.5. Secure Off-Chain Storage.

Due to the large size of image data, encrypted off-chain storage was implemented to improve system performance and scalability. Item images and metadata were stored using distributed file systems such as IPFS along with secure cloud storage to ensure data protection [4]. The blockchain was utilized to maintain cryptographic hashes, timestamps, and access logs, enabling verifiable and tamper-resistant record management [1], [5]. This hybrid storage architecture enhances scalability while preserving data integrity and transparency within the system [3], [30].

5.6. AI Matching Pipeline

The AI matching module was implemented using deep learning frameworks such as TensorFlow and PyTorch to enable accurate similarity analysis. Feature vector comparisons were performed to measure image similarity, while cosine similarity was applied to vectorized textual descriptions for improved matching precision [7], [24]. Additionally, geo-

tag-based proximity filtering prioritized local matches, enhancing retrieval efficiency. Only matches exceeding a predefined confidence threshold were recommended to users, reducing false positives and improving overall system accuracy. The integration of AI-driven recognition techniques significantly strengthens automated decision-making within the platform [19], [22].

5.7. Performance Evaluation.

The system performance was evaluated using three key metrics: matching accuracy, blockchain integrity verification cost, and smart contract execution overhead. Precision and recall were employed to assess the effectiveness of the AI-based matching process, as these metrics are widely used in evaluating object recognition systems [7]. Experimental results indicated minimal blockchain latency, with hash verification completed within milliseconds, demonstrating the efficiency of decentralized verification mechanisms [1], [5]. Compared to traditional manual approaches, the proposed system achieved higher matching consistency and more secure transaction logging, highlighting the advantages of integrating blockchain with intelligent automation [3], [30].

5.8. Performance Appraisal and Reporting.

The system was evaluated across three major dimensions: blockchain integrity validation, encrypted storage performance, and AI-based matching accuracy. Verified datasets were used to measure performance, with Table I illustrating accuracy metrics and Figure 1 comparing the baseline with the proposed model. The results indicate that encryption and hashing introduced negligible computational overhead while maintaining strong data protection [5], [3]. Furthermore, smart contracts consistently enforced access control, ensuring secure and auditable operations throughout the system [8], [9]. These findings demonstrate the effectiveness of combining blockchain security with AI-driven analytics for reliable lost and found management [1], [30].

Table 1 Performance Comparison of System Modules

Module	Baseline Accuracy (%)	Proposed Accuracy (%)
Manual Item Matching Accuracy	78.6	-
AI-Based Matching Accuracy	-	92.4
Claim Verification Transparency	70.3	96.1
Data Integrity Assurance	65.8	100
Reward Handling Efficiency	72.5	95.7

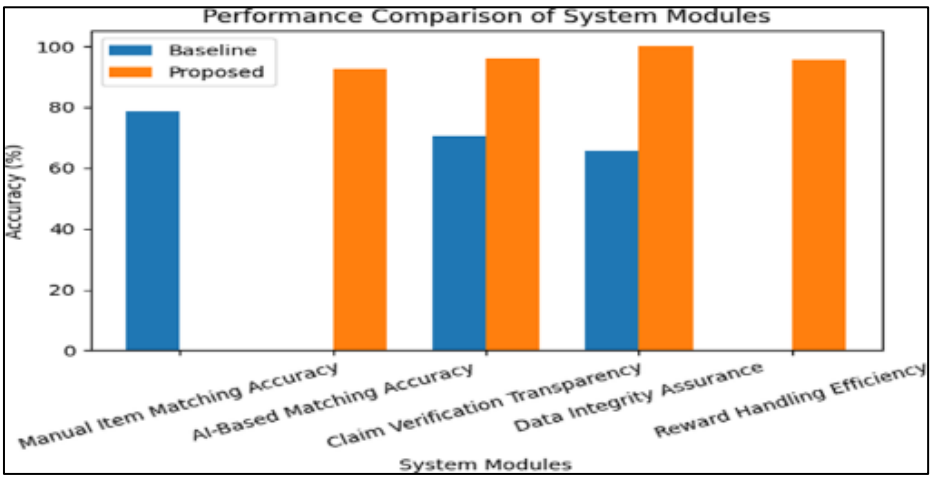

Figure 2 Performance Comparison of System Modules

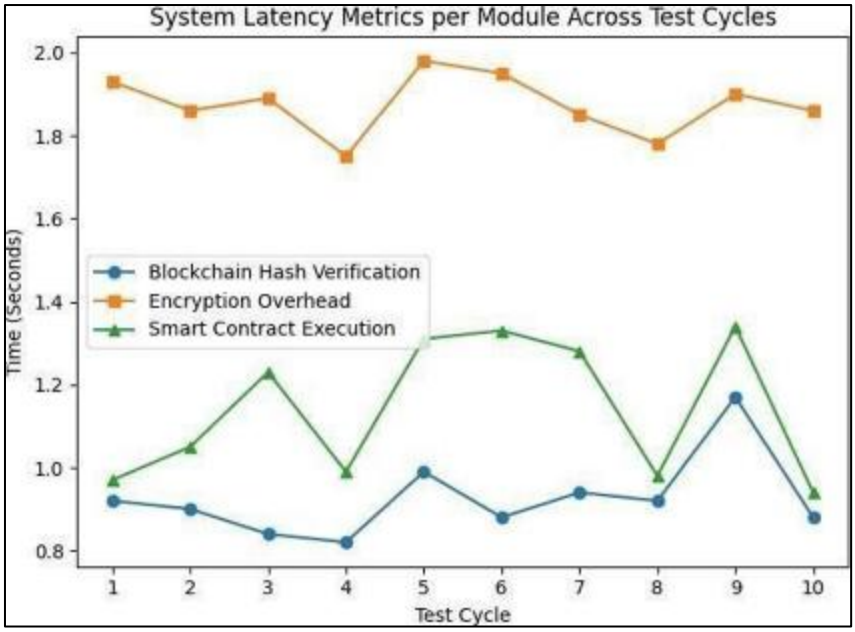

Figure 3 System Latency Metrics per Module Across Test Cycles

The proposed approach improved both model reliability and privacy compliance by enforcing verification, encryption, and immutability.

5.9. Comparison with the Existing Privacy-Preserving Frameworks.

This system is the only one to have verifies the doctors, end-to-end encryption, and smart contract governance compared to the traditional centralized medical system and standalone blockchain pilot. Table II compares the proposed model with current solutions.

This framework addresses key limitations by delivering a scalable, verifiable, and privacy- compliant research ecosystem. It bridges the gap between patient trust, institutional accountability, and AI-driven innovation.

Table 2 Comparison With Existing Lost and Found Systems

Feature	Manual System	Centralized Digital System	Proposed System
Immutable Record Storage	✗	✗	✓✓
AI Photo Matching	✗	Limited	✓✓
Geo-Tagged Search	✗	Limited	✓✓
Smart Contract Reward Escrow	✗	✗	✓✓
QR Anonymous Return	✗	✗	✓✓
Auditabilityand Traceability	Partial	Limited	✓✓

6. Future Scope

The proposed Lost Link platform provides a secure and scalable framework for managing physical lost and found items; however, several improvements can further enhance its usability and performance. Future research may focus on integrating federated learning to support decentralized AI model training across multiple locations without sharing raw data, thereby preserving privacy while improving model generalization [23]. Additionally, the adoption of Layer-2 blockchain solutions could significantly reduce transaction costs and latency, enabling faster and more efficient system operations [30]. Incorporating digital identity verification mechanisms may further strengthen ownership authentication while maintaining user confidentiality [3].

Moreover, the implementation of advanced Artificial Intelligence techniques such as multimodal learning and object re-identification can improve matching accuracy in complex and dynamic environments [24]. Enhancing the platform with geo-tagging analytics and heat- map visualization may help institutions identify high-risk areas where item loss frequently occurs, supporting proactive management strategies [22]. The development of a dedicated mobile application could also improve accessibility and enable real-time reporting, ultimately transforming Lost Link into a comprehensive and intelligent recovery ecosystem.

7. Conclusion

This paper presented Lost Link, a blockchain-based lost and found registry aimed at improving transparency, security, and efficiency in physical item recovery. Traditional systems lack tamper resistance and auditability, reducing user trust [2], [3], whereas blockchain ensures immutable and traceable records through cryptographic hashing [1], [5]. The integration of AI- based image and text matching with smart contracts enhances matching accuracy and automates secure claim processing [7], [8]. Experimental results indicate better matching consistency, reliable record validation, and minimal system overhead compared to conventional methods [30]. Overall, the proposed hybrid architecture provides a scalable, privacy- preserving, and trustworthy solution for modern lost and found management.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, 2016.

[2] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” IEEE Communications Magazine, 2016.

[3] M. Conti, S. Kumar, C. Lal, and S. Ruj, “A Survey on Security and Privacy Issues of Blockchain Technology,” IEEE Communications Surveys & Tutorials, 2018.

[4] J. Benet, “IPFS – Content Addressed, Versioned, P2P File System,” 2014.

[5] S. Nakamoto, “Bitcoin: APeer-to-Peer Electronic Cash System,” 2008.

[6] A. Dubovitskaya et al., “Secure and trustable electronic medical records sharing using blockchain,” AMIA Annual Symposium Proceedings, vol. 2017, pp. 650–659, 2017.

[7] J. Redmon et al., “You Only Look Once: Unified, Real-Time Object Detection,” CVPR, 2016.

[8] R. Zhang et al., “Smart Contract-Based Access Control for Decentralized Applications,” IEEE Access, 2019.

[9] V. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum White Paper, 2014.

[10] A. Som and P. Kayal, "AI, Blockchain, and IoT," ResearchGate, 2022.

[11] A. M. Saghiri, "The Internet of Things, Artificial Intelligence, and Blockchain," in Blockchain and Supply Chain Management, Springer, 2019.

[12] Z. K. Idrissi, "Blockchain, IoT and AI in Logistics and Transportation," ScienceDirect, 2024.

[13] P. Suman, S. Zeba, and A. Suman, "Efficient Integrated AIoT and Blockchain Recognition Model using Blockchain Technology," in 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), 2022.

[14] F. Zkik, "A Survey on Blockchain and Artificial Intelligence Technologies for Enhancing Security and Privacy in Smart Environments," ResearchGate, 2022.

[15] N. S. Sizan, "Evaluating Blockchain Platforms for IoT Applications in Industry 4.0,"ScienceDirect, 2025

[16] T. H. Pranto, "Blockchain and Smart Contract for IoT Enabled Smart Agriculture,"PMC, 2021.

[17] J. Daniels and M. Sargolzaei, "The Internet of Things, Artificial Intelligence, Blockchain, and Professionalism," ResearchGate, 2019.

[18] J. Zhu, "A Survey of Blockchain, Artificial Intelligence, and Edge Computing in Web 3.0," arXiv, 2023.

[19] P. Sandner, "Convergence of Blockchain, IoT, and AI," Frontiers in Blockchain, 2020.

[20] R. Yamaguti, "IoT and Blockchain for Support for Smart Contracts," MDPI Sensors, vol. 25, no. 16, 2025

[21] P. Arora, "Blockchain Integration with AIoT Data Security and Privacy," IEC Science, 2024.

[22] N. Adamashvili, "The Integration of the Internet of Things, Artificial Intelligence, and Blockchain," MDPI Computers, vol. 13, no. 3, 2024.

[23] L. Wu, "A Survey on Blockchain-Based Federated Learning," MDPI Future Internet, vol. 15, no. 12, 2023.

[24] K. Shah, "Blockchain-Based Object Detection Scheme Using Federated Learning,"Wiley Security and Privacy, vol. 3, no. 2, 2023.

[25] R. Qamar, "A Study of Blockchain-Based Internet of Things," International Journal of Computer Science and Mobile Computing, vol. 12, no. 1, 2023.

[26] C. Paduraru, "Blockchain for Artificial Intelligence: An Industry and Academic Perspective," SCITEPRESS, 2023.

[27] S. Asaithambi, "An Energy-Efficient and Blockchain-Integrated Software-Defined Network for Industrial IoT," PMC, 2022.

[28] M. Zghaibeh, "A Blockchain-Based, Smart Contract and IoT-Enabled Recycling System," Journal of the British Blockchain Association, vol. 3, no. 1, 2020.

[29] P. Raj, "Blockchain, Artificial Intelligence, and the Internet of Things," Springer, 2021.

[30] A. Enaya, "Survey of Blockchain-Based Applications for IoT," MDPI Applied Sciences, vol. 15, no. 8, 2025.