International Journal of Computer, Information Technology and Artificial Intelligence (IJCITAI)

مجله بین‌المللی کامپیوتر، فناوری اطلاعات و هوش مصنوعی

https://ijcitai.ir

دوره ۱ – شماره ۱ (پاییز ۱۴۰۴) – صفحه ۴۹ تا ۶۰

Convergence of Artificial Intelligence, Internet of Things, and Blockchain in Human-Centric Industry ۵،۰ Enabling Systematic Review, Conceptual Architecture, and Strategic Roadmap

Alireza joshan[۱]

[۱] Master of Science in Electrical Power Engineering, Faculty of Electrical Engineering, University of Guilan, Guilan, Iran,Alireza.joshan.guilan@gmail.com

Abstract

Industry ۵،۰ envisions an industrial paradigm that is not only automated, but human-centric, sustainable, and resilient. The convergence of Artificial Intelligence (AI), Internet of Things (IoT), and Blockchain offers a powerful technological foundation to realize this vision. In this paper, we present a conceptual architecture for their integration, conduct a systematic review of existing literature (including design patterns, use cases, and barriers), and analyze real-world examples. We identify the most significant technical, governance, and scalability challenges, and propose a multi-phase roadmap for deployment. Finally, we outline future research directions, such as post-quantum blockchains, federated learning, and autonomous economic agents. Our analysis suggests that while this tri-technology convergence holds transformative potential, practical adoption requires careful design, policy frameworks, and iterative prototyping.

Keywords: Industry ۵،۰, Artificial Intelligence, Internet of Things, Blockchain, Architecture, Roadmap.

دوره ۱ – شماره ۱ (پاییز ۱۴۰۴) – صفحه ۴۹ تا ۶۰

I. Introduction

The concept of Industry ٥,٠ represents the next evolutionary step in industrial transformation. Unlike Industry ٤,٠, whose primary emphasis lay on automation, connectivity, and efficiency, Industry ٥,٠ places humans at the center of industrial processes, stressing sustainability, collaboration, and system resilience(Sandner et al.,٢٠٢٠). In practical terms, this means integrating intelligent IoT devices with advanced decision-making (AI) under a trustworthy and decentralized infrastructure (blockchain) to establish a new generation of socio-technical systems(Aravinth,٢٠٢٥ ;Atlam et al.,٢٠٢٠).

IoT devices generate vast streams of real-time data from machines, environments, and human interactions. However, such data is often siloed, vulnerable, or untrusted unless appropriately secured and managed. Blockchain can address these limitations by providing an immutable, distributed ledger, enabling smart contracts, secure data provenance, and decentralized trust(Leng et al.,٢٠٢٢ ;Rejeb et al.,٢٠٢٥). In parallel, AI techniques ranging from edge-based machine learning to federated learning extract actionable insights from IoT data, enabling predictive maintenance, real-time anomaly detection, and adaptive decision-making.

When combined, these technologies make possible autonomous economic agents IoT devices that can transact, negotiate, and self-govern through blockchain-mediated contracts, while leveraging AI for intelligent behavior. This paradigm has been theorized by several works and offers compelling prospects for Industry ٥,٠ systems (Choi et al.,٢٠٢٤ ;Taherdoost et al.,٢٠٢٢ ;Aounzou et al.,٢٠٢٥ ;Azad et al.,٢٠٢٥ ;Rehman et al.,٢٠٢٢).

Yet, realizing this convergence in real-world industrial settings is non-trivial. IoT devices are frequently resource-constrained (compute, energy, memory), blockchain networks may face scalability and latency issues, and AI models often lack transparency and governance. Furthermore, deploying such systems demands robust policy frameworks: data ownership, identity management, accountability, and legal compliance must be addressed.

In this paper, we provide a structured and detailed examination of these issues. Our contributions are: (١) a layered conceptual architecture for AI–IoT–Blockchain integration; (٢) critical review of the literature with comparison of major works; (٣) real-world and near-future deployment examples; (٤) a multi-phase roadmap for practical adoption; and (٥) identification of future research directions aligned with Industry ٥,٠ goals.

٢.Systematic Review Methodology (PRISMA-Based)

٢,١. Review Design

This research was conducted as a systematic literature review following the PRISMA ٢٠٢٠ guidelines. The primary objective was to identify and synthesize scientific studies addressing the convergence of Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain within the context of Industry ٥,٠.

٢,٢. Data Sources and Search Strategy

A structured search was performed across the following scientific databases:

١.Scopus

٢.Web of Science

٣.IEEE Xplore

IJCITAI
International Journal of Computer, Information Technology and Artificial Intelligence (IJCITAI)

مجله بین‌المللی کامپیوتر، فناوری اطلاعات و هوش مصنوعی

https://ijcitai.ir

دوره ۱ – شماره ۱ (پاییز ۱۴۰۴) – صفحه ۴۹ تا ۶۰

٤.ScienceDirect

Timeframe:

January ٢٠١٥ to January ٢٠٢٥

Sample Search Terms:

"Industry ٥,٠," "AI and IoT," "AI and Blockchain,"
"IoT and Blockchain," "technology convergence,"
"human-centric industry," "cyber-physical systems."

Only peer-reviewed journal articles and conference papers written in English were considered.

٢,٣. Inclusion and Exclusion Criteria

Inclusion Criteria

١.Direct relevance to Industry ٥,٠ or human-centric industrial paradigms

٢.Examination of at least two of the three technologies (AI, IoT, Blockchain)

٣.Full-text availability

٤.Peer-reviewed scientific publications

٥.English-language studies

Exclusion Criteria

١.Studies focused solely on Industry ٤,٠ without explicit linkage to Industry ٥,٠

٢.Purely conceptual papers lacking practical or technological integration

٣.Duplicate publications

٤.Studies that did not address technological convergence

٢,٤. Study Selection Process (PRISMA Flow)

Phase ١ — Identification

A.Total records identified: ٢٦٥

Phase ٢ — Screening

A.Duplicates removed: ٦١

B.Remaining after deduplication: ٢٠٤

دوره ۱ – شماره ۱ (پاییز ۱۴۰۴) – صفحه ۴۹ تا ۶۰

C.Title and abstract screening removed: ١٣٤

Phase ٣ — Eligibility

A.Full-text articles assessed: ٧٠

B.Excluded after full-text review: ٤٥
(due to insufficient relevance or lack of multi-technology integration)

Phase ٤ — Included

A.Studies included in the final synthesis:
٢٥ articles

PRISMA Summary

A.Records identified: ٢٦٥

B.Duplicates removed: ٦١

C.Screened records: ٢٠٤

D.Full texts assessed: ٧٠

E.Final included studies: ٢٥

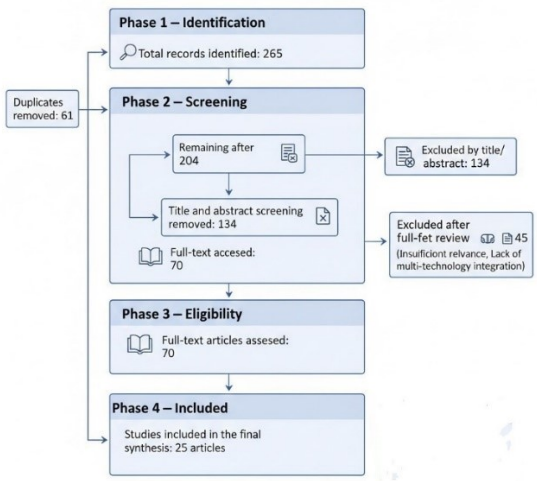

Figure١. PRISMA Flow Diagram of the Methodology

٢,٥. Data Extraction and Analysis

For each of the ٢٥ included studies, the following information was extracted:

١.Application domain

٢.Type and depth of AI–IoT–Blockchain convergence

٣.Alignment with Industry ٥,٠ principles (human-centricity, resilience, sustainability)

٤.Challenges, benefits, models, and frameworks proposed

A qualitative content analysis approach was used to synthesize key themes and identify knowledge gaps and future research opportunities.

٢,٦. Research Limitations

١. Use of only four major databases may have limited coverage.
٢. Restriction to English-language studies.
٣. Timeframe limited to ٢٠١٥–٢٠٢٥.
٤. Possible exclusion of borderline studies during screening.
٥. Industry ٥,٠ remains an emerging field with limited academic maturity.
٦. Heterogeneity of methodologies and application domains across the studies.
٧. Qualitative synthesis introduces potential interpretive bias.
٨. A meta-analysis was not feasible due to methodological and conceptual diversity.

٣. Conceptual Architecture

To guide the design and implementation of converged AI–IoT–Blockchain systems for Industry ٥,٠, we propose a six-layer conceptual architecture (Figure ٢) that ensures trust, intelligence, autonomy, and human-centric oversight:

١. Sensing Layer (IoT): This layer comprises sensors, actuators, and edge devices deployed across industrial systems to collect real-time data, such as vibration, temperature, and operational usage. The sensing layer serves as the foundation for all subsequent processing and decision-making.
٢. Edge & Preprocessing Layer: Edge computing nodes perform preprocessing tasks, including data filtering, aggregation, and compression. This reduces communication costs and latency, while ensuring that only relevant data is transmitted to higher layers for advanced analysis.
٣. Trust Layer (Blockchain): A distributed ledger, which can be permissioned or hybrid, records critical IoT transactions. It supports smart contracts and ensures data immutability, enabling secure, decentralized, and verifiable interactions among devices.
٤. Intelligence Layer (AI): AI and machine learning models, deployed on edge or cloud platforms, analyze IoT data to enable predictive maintenance, anomaly detection, and operational optimization. This layer transforms raw data into actionable insights for decision-making.
٥. Learning & Collaboration Layer: Federated learning or blockchain-backed collaborative learning enables decentralized model training across multiple devices or organizations, preserving data privacy while improving model accuracy and generalizability.
٦. Governance & Agent Layer: Devices act as autonomous agents, transacting via smart contracts. Governance policies regulate identities, permissions, and accountability, ensuring that human oversight is maintained while enabling decentralized operations.

This architecture aligns with the human-centric goals of Industry ٥,٠, providing trust, intelligence, and autonomy, while maintaining human oversight through governance mechanisms. As illustrated in Figure ٢,

IJCITAI
International Journal of Computer, Information Technology and Artificial Intelligence (IJCITAI)
مجله بین‌المللی کامپیوتر، فناوری اطلاعات و هوش مصنوعی
https://ijcitai.ir
دوره ۱ – شماره ۱ (پاییز ۱۴۰۴) – صفحه ۴۹ تا ۶۰

this converged AI–IoT–Blockchain architecture serves as a blueprint for designing resilient, secure, and intelligent industrial systems.

Figure٢.A Converged AI-IoT-Blochchain Architecture for Trust,intelligence,and Autonomy in Industry٥،٠

٤. Literature Review

٤،١. Key Research Contributions

Over the past decade, significant research has explored the convergence of Artificial Intelligence (AI), the Internet of Things (IoT), and Blockchain, particularly within the context of Industry ٥،٠. Atlam et al. (٢٠٢٠) provided a foundational review demonstrating how blockchain integration with IoT can enhance trust and data security, while AI further addresses scalability challenges and facilitates intelligent decision-making in decentralized industrial environments. Building upon this, Leng et al. (٢٠٢٢) proposed a detailed architecture for secure blockchain middleware in Industrial IoT (IIoT), outlining enablers and challenges that are specific to Industry ٥،٠ use cases, thereby providing practical guidance for system designers. Rejeb et al. (٢٠٢٥) employed co-word and topic modeling analyses to highlight the interplay between blockchain, AI, IoT, and circular economy principles, revealing research gaps and emerging trends in the field. Choi and Kim (٢٠٢٤) further examined the technological convergence of AI and blockchain, identifying critical bottlenecks such as data reliability and cross-platform compatibility, and proposed a structured research framework to overcome these limitations.

Practical applications have also been a focus of recent studies. Taherdoost (٢٠٢٢) critically reviewed AI–blockchain deployments across multiple domains, emphasizing integration risks and obstacles to large-scale implementation. Similarly, Aounzou et al. (٢٠٢٥) conducted a systematic review of blockchain, IoT, and machine learning applications, mapping key opportunities and real-world challenges for industrial systems. Innovative solutions such as quantum-resistant blockchain protocols have been proposed by Azad et al. (٢٠٢٥) to enhance IoT consensus mechanisms, ensuring resilience against potential attacks. Rehman et al. (٢٠٢٢) demonstrated a secure Healthcare ٥،٠ system that couples federated learning with blockchain to preserve privacy in IoT-enabled medical networks, highlighting the importance of decentralized intelligence and secure data handling. Furthermore, Jahid et al. (٢٠٢٣) explored the convergence of blockchain, IoT, and ٦G networks, emphasizing how next-generation connectivity can support scalable, intelligent, and decentralized industrial systems. Finally, Conoscenti, Vetro, and De Martin (٢٠١٦) systematically reviewed

IJCITAI
International Journal of Computer, Information Technology and Artificial Intelligence (IJCITAI)
مجله بین‌المللی کامپیوتر، فناوری اطلاعات و هوش مصنوعی
https://ijcitai.ir
دوره ۱ – شماره ۱ (پاییز ۱۴۰۴) – صفحه ۴۹ تا ۶۰

blockchain applications for IoT, providing a taxonomy and identifying architectural patterns that continue to inform contemporary system design.

Taken together, these studies collectively demonstrate that while the conceptual foundations and technical prototypes for AI–IoT–Blockchain convergence are well-established, practical deployment in Industry ٥,٠ remains constrained by challenges such as integration complexity, scalability, and governance. Moreover, gaps in real-world implementations, secure collaborative learning, and quantum-resistant solutions highlight opportunities for future research, underscoring the critical need for frameworks that bridge theory and practice in designing human-centric, intelligent, and resilient industrial systems.

٤,٢. Comparison of Selected Works

Table١. Comparative Review of Selected Studies

Ref	Technologies	Focus/Use Case	Key Achievements	Limitations
Atlam et al.,٢٠٢٠[٣]	Blockchain + IoT + AI	IoT architectures and trust	Offers a structured survey and identifies future directions	Limited empirical evaluation of combined systems
Leng et al.,٢٠٢٢[٤]	Blockchain + IIoT	Middleware for IIoT	Proposes a secure middleware architecture tailored to Industry ٥,٠	Focuses more on blockchain than AI or learning
Rejeb et al.,٢٠٢٥[٥]	Blockchain + IoT + AI	Bibliometric / thematic analysis	Reveals trends in sustainability and human-machine collaboration	Less on systems implementation
Choi et al.,٢٠٢٤[٦]	Blockchain + AI	Convergence challenges	Thorough analysis of technical issues such as scalability and data integrity	Does not deeply address IoT resource constraints
Taherdoost ,٢٠٢٢[٧]	Blockchain + AI	Application review	Broad coverage of use cases and risks	High-level; lacks deployment best practices
Aounzou et al.,٢٠٢٥[٨]	Blockchain + IoT + ML	Systematic review	Highlights ML-based solutions and integration barriers	Limited focus on runtime performance
Azad et al.,٢٠٢٥[٩]	Blockchain (quantum) + IoT	Voting consensus	Proposes quantum-resistant consensus for IoT	Experimental / simulated, not yet deployed at scale
Rehman et al.,٢٠٢٢[١٠]	Blockchain + Federated Learning + IoT	Healthcare systems	Ensures privacy and trust in distributed medical IoT	Complexity in real-world regulatory compliance
Jahid et al.,٢٠٢٣[١١]	Blockchain + IoT + ٦G	Network convergence	Vision of future ٦G-enabled decentralized systems	٦G is still speculative in many regions
Conoscenti et al.,٢٠١٦[١٢]	Blockchain + IoT	Taxonomy and applications	Defines architectural patterns and use cases	Does not cover AI integration deeply

٥. Real-World Deployment Examples

Recent real-world deployments illustrate the practical potential of converged AI–IoT–Blockchain systems in Industry ٥,٠. Azad et al. (٢٠٢٥) implemented a quantum-resistant blockchain voting protocol in a simulation environment for IoT devices, demonstrating a viable approach toward secure post-quantum consensus in industrial networks. This work highlights the importance of integrating quantum-safe mechanisms to protect decentralized industrial systems against emerging cyber threats. In the Healthcare ٥,٠ domain, Rehman et al.

(٢٠٢٢) combined IoT medical sensors, federated learning, and blockchain technologies to develop a privacy-preserving health monitoring system. Their deployment exemplifies how decentralized intelligence and secure data management can be achieved in sensitive environments, ensuring both patient privacy and real-time monitoring. Additionally, Leng et al. (٢٠٢٢) proposed a middleware architecture that aligns closely with industrial deployments requiring secure, decentralized Industrial IoT (IIoT). This architecture supports predictive maintenance and real-time coordination among heterogeneous devices, demonstrating the practical applicability of AI–IoT–Blockchain convergence in complex industrial environments. Collectively, these examples underscore that while conceptual frameworks are essential, the successful realization of Industry ٥،٠ systems depends on carefully designed, secure, and human-centric deployments capable of integrating emerging technologies into operational settings.

٦. Critical Analysis

The integration of AI, IoT, and blockchain in Industry ٥،٠ presents multiple critical challenges that must be addressed to achieve scalable, secure, and human-centric systems. Scalability and performance remain primary concerns, as many blockchain consensus mechanisms impose significant computational overhead that exceeds the capabilities of typical IoT devices. While middleware solutions can partially alleviate these limitations, further optimization is necessary to ensure efficient operation in large-scale deployments (Leng et al., ٢٠٢٢; Aounzou et al., ٢٠٢٥). Resource constraints pose an additional barrier, since IoT nodes generally have limited CPU, memory, and energy resources. Integrating AI and blockchain under such constrained conditions is particularly challenging and requires careful design choices to maintain performance without exhausting resources (Choi et al., ٢٠٢٤; Khan et al., ٢٠٢٥).

Governance and autonomy are also critical, especially as autonomous economic agents IoT devices capable of transacting independently raise questions regarding accountability, identity management, and regulatory compliance. Addressing these issues is essential to ensure that decentralized operations remain transparent and aligned with human-centric objectives (Sandner et al., ٢٠٢٠; Rejeb et al., ٢٠٢٥; Ghaderi et al., ٢٠٢٥). Security and privacy tensions further complicate implementation, as blockchain's inherent transparency may conflict with privacy requirements in sensitive domains such as healthcare. Federated learning can help mitigate some privacy concerns, yet governance frameworks to manage access, consent, and accountability are still underdeveloped (Rehman et al., ٢٠٢٢; Singh et al., ٢٠٢٠; Nguyen et al., ٢٠٢٤).

Finally, future-proofing these systems remains a significant challenge. Emerging quantum-resistant protocols, such as blockchain-based voting schemes, demonstrate promising security properties against potential post-quantum threats. However, practical deployment, interoperability, and real-world adoption of these solutions are still immature and require further research and rigorous testing (Azad et al., ٢٠٢٥). Collectively, these challenges underscore the need for integrated design strategies, robust governance models, and continued innovation to realize the full potential of AI–IoT–Blockchain convergence in Industry ٥،٠.

٧. Deployment Roadmap

The deployment of AI–IoT–Blockchain convergence in Industry ٥،٠ can be structured into seven sequential phases, each targeting specific technical, governance, and operational objectives. This roadmap integrates insights from prior studies and provides actionable steps for researchers and industrial practitioners (Fraga-Lamas et al., ٢٠١٩; Khan et al., ٢٠٢٥; Sizan et al., ٢٠٢٥; Tyagi et al., ٢٠٢٤; Bhumichai et al., ٢٠٢٤; Sait et al., ٢٠٢٥; Zhang et al., ٢٠٢١; Luo et al., ٢٠٢٤ ;Mololoth et l.,٢٠٢٣ ;Rajawat et al.,٢٠٢٢).

The first phase, Readiness Assessment, involves evaluating existing infrastructure, inventorying IoT devices, edge computing capabilities, and network latency, to identify feasibility gaps and prepare for integration. Phase two, Architecture Design, focuses on defining the system architecture, selecting the appropriate blockchain type, AI deployment mode (edge or cloud), and smart contract templates, thus producing a blueprint for integration. In the Proof-of-Concept (PoC) phase, a pilot system is built by integrating IoT sensors, blockchain ledgers, and simple AI models to validate workflows, assess latency, and ensure trustworthiness.

The Federated Learning phase deploys privacy-preserving collaborative AI models coordinated with blockchain, enabling decentralized intelligence while protecting sensitive data. In parallel, the Governance Framework phase establishes policies for identity management, access control, accountability via smart contracts, and regulatory and ethical compliance. Scale-up involves expanding the system, optimizing consensus mechanisms, refining AI models, and integrating additional devices to achieve production-ready, robust operations. Finally, the Continuous Monitoring & Evolution phase tracks key performance indicators such as latency, accuracy, and energy consumption, maintaining system efficiency while incorporating new technologies and iterative improvements.

These seven phases collectively provide a structured, actionable roadmap for realizing practical, secure, and scalable AI–IoT–Blockchain deployments in Industry ٥,٠. The detailed phase-wise summary is presented in Table ٢.

Table ٢. Roadmap Summary Table

Phase	Description	Key Actions	Expected Outcome
١. Readiness Assessment	Evaluate existing infrastructure and IoT capabilities	Inventory IoT devices, edge nodes, network latency	Determine feasibility, identify system gaps
٢. Architecture Design	Define system architecture	Select blockchain type, AI deployment mode (edge/cloud), smart contract templates	Blueprint for integration
٣. Proof-of-Concept (PoC)	Build pilot system	Integrate IoT sensors, blockchain ledger, simple AI models	Validate workflow, assess latency, ensure trust
٤. Federated Learning	Deploy decentralized collaborative AI	Implement federated learning with blockchain coordination	Privacy-preserving, collaborative AI models
٥. Governance Framework	Establish rules and compliance	Identity management, access control, accountability via smart contracts	Regulatory and ethical compliance
٦. Scale-up	Expand and optimize system	Optimize consensus, refine AI, integrate more devices	Production-ready, robust system
٧. Continuous Monitoring & Evolution	Maintain and evolve system	Track KPIs (latency, accuracy, energy), upgrade blockchain/AI	Maintain efficiency, incorporate new technologies

٨. Future Research Directions

Recent advances in the convergence of Artificial Intelligence, Internet of Things, and Blockchain in Industry ٥,٠ highlight several critical research directions that require further exploration. First, post-quantum blockchain represents a key challenge and opportunity. Developing quantum-resistant consensus protocols, such as blockchain-based voting schemes, is essential for industrial IoT networks to ensure security and trust against emerging post-quantum threats (Azad et al., ٢٠٢٥).

In the AI domain, Explainable AI (XAI) is of paramount importance. As industrial systems increasingly rely on autonomous agents performing independent transactions, AI models must be auditable and transparent. This not only enhances human trust but also enables proper governance and accountability in autonomous decision-making.

Interoperability standards constitute another critical research need. Standard protocols for cross-chain and cross-platform communication among blockchain networks, IoT devices, and AI frameworks are required to support scalability, multi-platform integration, and efficient system management. Such standards facilitate seamless operation in complex industrial ecosystems.

Beyond technical aspects, regulatory and policy research is essential to develop governance models and legal frameworks for autonomous agents operating in industrial environments. Proper policy frameworks are necessary to ensure accountability, transparency, and compliance, especially in multi-stakeholder and multi-organizational industrial networks.

Finally, sustainability is a core objective of Industry ۵,۰. Future research should focus on energy-efficient consensus mechanisms and AI models that align with environmental goals, reducing resource consumption while maintaining system performance (Rejeb et al., ۲۰۲۵; Gadekallu et al., ۲۰۲۱; Alharbi et al., ۲۰۲۲).

From an operational perspective, the successful advancement of these directions requires pilot testing, simulation models, and interdisciplinary collaboration among AI engineers, network specialists, and policy-makers. Furthermore, designing measurable tools to evaluate performance, energy consumption, security, and interoperability will facilitate the translation of these research directions into practical, production-ready solutions for Industry ۵,۰ systems.

۹. Conclusion

The integration of Artificial Intelligence, the Internet of Things, and Blockchain provides a powerful and innovative foundation for realizing the vision of human-centric, intelligent, and decentralized Industry ۵,۰ systems. A systematic review of the literature and analysis of real-world examples indicate that, although significant conceptual progress and promising prototypes have been developed, practical adoption in industrial environments requires overcoming technical constraints such as scalability, resource consumption, and integration complexity. Moreover, the design and implementation of effective governance models, standardization of protocols, and alignment with future-ready technologies such as quantum-safe blockchains, federated learning, and autonomous economic agents are critical for success. By following a phased roadmap, emphasizing conceptual architecture, design analysis, and iterative system deployment, this tri-technology convergence can serve as a practical driver of the next industrial revolution, paving the way for the development of intelligent, resilient, reliable, and human-centric industrial systems. This approach not only enables higher efficiency and data-driven decision-making but also facilitates the advancement of cutting-edge technologies and science- and industry-informed policy frameworks.

References

١. Sandner, P., Gross, J., & Richter, R. (٢٠٢٠). *Convergence of Blockchain, IoT, and AI*. Frontiers in Blockchain, ٣, ٥٢٢٦٠٠. https://doi.org/١٠,٣٣٨٩/fbloc.٢٠٢٠,٥٢٢٦٠٠

٢. Aravinth, S. S. (٢٠٢٥). Unleashing the power of data and security by integrating deep learning and blockchain in smart city infrastructure development–A future perspective. In *Deep Learning and Blockchain Technology for Smart and Sustainable Cities* (pp. ٢٠–٤٢). Auerbach Publications. https://doi.org/١٠,١٢٠١/٩٧٨١٠٠٣٤٧٦٠٤٧

٣. Atlam, H. F., Azad, M. A., Alzahrani, A. G., & Wills, G. (٢٠٢٠). A review of blockchain in Internet of Things and AI. *Big Data and Cognitive Computing, 4*(٤), ٢٨. https://doi.org/١٠,٣٣٩٠/bdcc٤٠٤٠٠٢٨

٤. Leng, J., Chen, Z., Huang, Z., Zhu, X., Su, H., Lin, Z., & Zhang, D. (٢٠٢٢). Secure blockchain middleware for decentralized IIoT towards Industry ٥,٠: A review of architecture, enablers, challenges, and directions. *Machines, 10*(١٠), ٨٥٨. https://doi.org/١٠,٣٣٩٠/machines١٠١٠٠٨٥٨

٥. Rejeb, A., Rejeb, K., Zrelli, I., & Süle, E. (٢٠٢٥). Industry ٥,٠ as seen through its academic literature: An investigation using co-word analysis. *Circular Economy and Sustainability*. https://doi.org/١٠,١٠٠٧/s٤٣٦١٥-٠٢٥-٠٠٥٧٠-y

٦. Choi, N., & Kim, H. (٢٠٢٤). Technological convergence of blockchain and artificial intelligence: A review and challenges. *Electronics, 14*(١), ٨٤. https://doi.org/١٠,٣٣٩٠/electronics١٤٠١٠٠٨٤

٧. Taherdoost, H. (٢٠٢٢). Blockchain technology and artificial intelligence together: A critical review on applications. *Applied Sciences, 12*(٢٤), ١٢٩٤٨. https://doi.org/١٠,٣٣٩٠/app١٢٢٤١٢٩٤٨

٨. Aounzou, Y., Boulaalam, A., & Kalloubi, F. (٢٠٢٥). Convergence of blockchain, IoT, and machine learning: Exploring opportunities and challenges – A systematic review. *International Journal on Smart Sensing and Intelligent Systems, 18*(١). https://doi.org/١٠,٢٤٧٨/ijssis-٢٠٢٥-٠٠٠٢

٩. Azad, U., Behera, B. K., Song, H., & Farouk, A. (٢٠٢٥). A blockchain-based quantum binary voting for decentralized IoT towards Industry ٥,٠. *arXiv:2503.20247*. https://doi.org/١٠,٤٨٥٥٠/arXiv.٢٥٠٣,٢٠٢٤٧

١٠. Rehman, A., Abbas, S., Khan, M. A., Ghazal, T. M., Adnan, K. M., & Mosavi, A. (٢٠٢٢). A secure Healthcare ٥,٠ system based on blockchain technology entangled with federated learning technique. *Computers in Biology and Medicine, 150*, ١٠٦٠١٩. https://doi.org/١٠,١٠١٦/j.compbiomed

١١. Jahid, A., Alsharif, M. H., & Hall, T. J. (٢٠٢٣). The convergence of blockchain, IoT and ٦G: Potential, opportunities, challenges and research roadmap. *Journal of Network and Computer Applications, 217*, ١٠٣٦٧٧. https://doi.org/١٠,١٠١٦/j.jnca.٢٠٢٣,١٠٣٦٧٧

١٢. Conoscenti, M., Vetro, A., & De Martin, J. C. (٢٠١٦). Blockchain for the Internet of Things: A systematic literature review. In *Proceedings of the IEEE/ACS 13th International Conference on Computer Systems and Applications (AICCSA)*. https://doi.org/١٠,١١٠٩/AICCSA.٢٠١٦,٧٩٤٥٨٠٥

١٣. Gadekallu, T. R., Pham, Q.-V., Nguyen, D. C., Maddikunta, P. K. R., Deepa, N., Pathirana, P. N., Zhao, J., & Hwang, W.-J. (٢٠٢١). Blockchain for edge of things: Applications, opportunities, and challenges. *IEEE Internet of Things Journal, 9*(٢), ٩٦٤–٩٨٨. https://doi.org/١٠,١١٠٩/JIOT.٣١١٩٦٣٩

١٤. Singh, N., Singh, S., & Singh, S. J. (٢٠٢٠). Convergence of blockchain and artificial intelligence in IoT: A security analysis. *Sustainable Cities and Society, 62*. https://doi.org/١٠,١٠١٦/j.scs.٢٠٢٠,١٠٢٣٨٧

١٥. Fraga-Lamas, P., & Fernandez-Carames, T. M. (٢٠١٩). A review on blockchain technologies for an advanced and cyber-resilient automotive industry. *IEEE Access, 7*, ١٧٥٧٨–١٧٥٩٨. https://doi.org/١٠,١١٠٩/ACCESS.٢٠١٩,٢٨٩٥٣٠٢

١٦. Tyagi, A. K., Tripathi, K., Kukreja, S., Tiwari, S., & U., A. S. (٢٠٢٤). Blockchain enabled artificial intelligence for Industry ٥,٠: Vision, challenges and opportunities. *Journal of Autonomous Intelligence, 7*(٥). https://doi.org/١٠,٣٢٦٢٩/jai.v٧i٥,١٤٧٩

١٧. Khan, I. U., Al-Hammadi, M. H., & Ghafoor, A. (٢٠٢٥). Integrating AI, blockchain, and edge computing for zero-trust systems. *Journal of Smart IoT Security* (pre-print).

١٨. Bhumichai, D., Smiliotopoulos, C., Benton, R., Kambourakis, G., & Damopoulos, D. (٢٠٢٤). The convergence of artificial intelligence and blockchain: The state of play and the road ahead. *Information, 15*(٥). https://doi.org/١٠,٣٣٩٠/info١٥٠٥٠٢٦٨

١٩. Nguyen, T., Nguyen, H., & Gia, T. N. (٢٠٢٤). Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications. *Journal of Network and Computer Applications, 226*, ١٠٣٨٨٤. https://doi.org/١٠,١٠١٦/j.jnca.٢٠٢٤,١٠٣٨٨٤

٢٠. Sizan, N. S., Dey, D., Layek, M. A., et al. (٢٠٢٥). Evaluating blockchain platforms for IoT applications in Industry ٥,٠: A comprehensive review. *Blockchain Research and Applications*, ١٠٠٢٧٦. https://doi.org/١٠,١٠١٦/j.bcra.٢٠٢٥,١٠٠٢٧٦

٢١. Sait, S. A., & Vijesh, P. V. (٢٠٢٥). The role of AI, IoT and blockchain in enabling workplace sustainability and efficiency—An empirical analysis. *Journal of Emerging Markets and Management, 1*(٢), ٦٦–٨٠. https://doi.org/١٠,٦٣٣٨٥/jemm.v١i٢,١٥٩
٢٢. Alharbi, S., Attiah, A., & Alghazzawi, D. (٢٠٢٢). Integrating blockchain with artificial intelligence to secure IoT networks: Future trends. *Sustainability, 14*(٢٣), ١٦٠٠٢. https://doi.org/١٠,٣٣٩٠/su١٤٢٣١٦٠٠٢
٢٣. Ghaderi, Y., & Ghaderi, M. R. (٢٠٢٥). Navigating the future of smart cities: Addressing IoT challenges through blockchain solutions. *Information Systems and Smart City, 5*(١), Article ٢٣٣٤. https://doi.org/١٠,٥٩٤٠٠/issc٢٣٣٤
٢٤. Zhang, Z., Song, X., Liu, L., Yin, J., Wang, Y., & Lan, D. (٢٠٢١). Recent advances in blockchain and artificial intelligence integration: Feasibility analysis, research issues, applications, challenges, and future work. *Security and Communication Networks, 2021*, ١–١٥. https://doi.org/١٠,١١٥٥/٢٠٢١/٩٩٩١٥٣٥
٢٥. Luo, X., & Mahdjoubi, L. (٢٠٢٤). Towards a blockchain- and machine-learning-based framework for decentralised energy management. *Energy and Buildings, 303*, ١١٣٧٥٧. https://doi.org/١٠,١٠١٦/j.enbuild.٢٠٢٣,١١٣٧٥٧
٢٦. Mololoth, V. K., Saguna, S., & Åhlund, C. (٢٠٢٣). Blockchain and machine learning for future smart grids: A review. *Energies*, *16*(١), ٥٢٨. https://doi.org/١٠,٣٣٩٠/en١٦٠١٠٥٢٨
٢٧. Rajawat, A. S., Bedi, P., Goyal, S. B., Shaw, R. N., Ghosh, A., & Aggarwal, S. (٢٠٢٢). Ai and blockchain for healthcare data security in smart cities. In *AI and IoT for Smart City Applications* (pp. ١٨٥-١٩٨). Singapore: Springer Nature Singapore. https://doi.org/١٠,١٠٠٧/٩٧٨-٩٨١-١٦-٧٤٩٨-٣_١٢