International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 05 Sep-Oct; 2026 Page. No. 1114-1125

To cite this article: Dr. Hajera Fatima Khan (2026). BLOCKCHAIN BEYOND CRYPTOCURRENCY: A Critical Review of Technical Foundations, Cross-Sector Applications, and Adoption Priorities, International Journal of Research in Commerce and Management Studies (IJRCMS) 8 (5): 1114-1125 Article No. 924 Sub Id 1506

BLOCKCHAIN BEYOND CRYPTOCURRENCY: A Critical Review of Technical Foundations, Cross-Sector Applications, and Adoption Priorities

Dr. Hajera Fatima Khan

Accounting Department, University of Hail, Hail, Saudi Arabia

DOI: https://doi.org/10.38193/IJRCMS.2026.8566

ABSTRACT

Blockchain has developed from the ledger architecture associated with Bitcoin into a family of distributed systems being explored for digital identity, financial services, healthcare information exchange, supply-chain traceability, education credentials, public administration, and energy coordination. Yet its value is not automatic: the same features that support shared verification and tamper-evident records can introduce performance costs, privacy tensions, governance complexity, and implementation burdens. This narrative review synthesizes four supplied publications addressing blockchain's technical mechanisms, historical development, research trends, sectoral uses, and continuing limitations. It considers distributed ledger architecture, cryptographic hashing, digital signatures, consensus protocols, and smart contracts as interdependent design elements rather than isolated features. The review compares potential benefits across sectors and argues that the strongest use cases are those in which multiple independent parties need a shared, auditable record and cannot fully rely on one organization's database. It also identifies conditions under which conventional databases may remain more suitable. Key priorities include scalable and energy-aware architectures, interoperability, privacy-by-design, secure contract development, clear accountability, regulatory alignment, and empirical evaluation of costs and outcomes. The paper concludes that responsible blockchain adoption should be driven by a demonstrable coordination problem and measurable public or organizational value—not by the novelty of the technology alone.

KEYWORDS: blockchain; distributed ledger technology; smart contracts; interoperability; privacy; supply-chain traceability; digital governance

1. INTRODUCTION

Blockchain emerged in association with Bitcoin, introduced through the 2008 proposal attributed to Satoshi Nakamoto. Its initial significance was the coordination of transactions among participants without requiring a single central intermediary to maintain the authoritative ledger. Over time, research and development moved beyond digital currency toward programmable platforms,

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 05 Sep-Oct; 2026 Page. No. 1114-1125

decentralized applications, and organizational systems. The introduction of smart-contract functionality broadened the design space by allowing rules to be executed through code and recorded as part of a shared transaction history (Mondal & Goswami, 2024; Singh, 2025).

The appeal of blockchain rests on a combination of distributed record keeping, cryptographic verification, consensus among network participants, and resistance to undetected retrospective alteration. These characteristics can support auditability and coordination when parties have different interests or limited mutual trust. Applications have consequently been suggested in different sectors like finance, healthcare, education, government services, scientific research, logistics, energy markets, and Internet of Things (IoT) environments (Saray & Kaplan, 2026; López-Sorribes et al., 2023).

However, a tamper-evident record is not necessarily a truthful record: inaccurate information entered at the point of collection can remain verifiably inaccurate. Nor does decentralization eliminate the need for accountability, legal remedies, data protection, or reliable system administration. This review therefore treats blockchain as a design choice with benefits and trade-offs, rather than a universal replacement for conventional information systems.

The conceptual framework of this study is constructed by considering the core components of blockchain technology, its sectoral applications, associated benefits, and prevailing challenges. Figure 1 conceptually summarizes the multi-sectoral nature of blockchain technology and the interactions among these sectors.

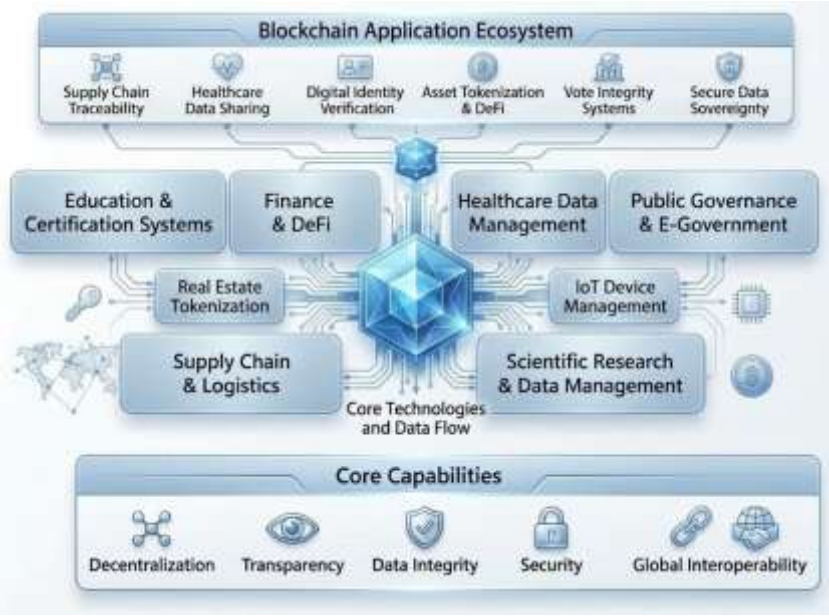


Figure 1: Block Chain Application Ecosystem.

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 05 Sep-Oct; 2026 Page. No. 1114-1125

Figure 1 presents a Block Chain Application Ecosystem explaining the core blockchain architecture and its applications across multiple sectors, together with the shared technical and governance-related challenges associated with these applications. The figure provides a holistic overview of how blockchain technology is positioned within finance, healthcare, education, public administration, scientific research, and supply chain management. Additionally, it highlights fundamental cross-sectoral issues such as scalability, energy efficiency, privacy concerns, and regulatory compliance.

The proposed conceptual framework guides the overall structure of this study and serves as a roadmap for the sector-specific analyses discussed in the subsequent sections.

2. AIM AND REVIEW QUESTIONS

The aim is to integrate the supplied literature into a critical overview of blockchain's technical basis, application landscape, limitations, and future priorities. Four questions guide the discussion: (1) Which technical mechanisms enable shared verification? (2) How has the technology's purpose expanded beyond cryptocurrency? (3) What benefits and constraints recur across sectoral applications? and (4) Which design and governance priorities could support responsible adoption?

3. REVIEW APPROACH

This manuscript uses a narrative synthesis of four user-provided publications: a 2026 cross-sector review, a 2025 technical overview available as an arXiv preprint, a 2023 bibliometric analysis, and a 2024 review of applications and future directions. The sources were read for recurring themes concerning architecture, evolution, applications, challenges, and proposed research directions. Findings are organized thematically and compared across the sources rather than pooled statistically. The paper does not claim to be a systematic review: it does not independently search all databases, apply a registered protocol, or reproduce the source studies' screening procedures. Its conclusions are interpretive and should be read within that scope.

4. TECHNICAL FOUNDATIONS

4.1 Distributed ledgers and cryptographic integrity

In a blockchain network, copies of a ledger are maintained across multiple nodes. Transactions are grouped into blocks, and blocks reference earlier blocks through cryptographic hashes. This linkage makes changes to historical data detectable because an alteration changes the corresponding hash and disrupts the expected chain. Digital signatures provide a way to verify that a transaction was authorized by the holder of a relevant private key, while hash-based structures can support efficient verification of transaction inclusion (Singh, 2025).

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 05 Sep-Oct; 2026 Page. No. 1114-1125

These mechanisms provide integrity and auditability, but they do not guarantee confidentiality. Depending on the network design, transaction details or patterns may be visible to participants. Sensitive records therefore require careful choices about what is written to the ledger, who can access it, and how identity and permissions are managed. A practical design may store only hashes, references, or permission records on-chain while keeping detailed personal or commercial information in appropriately governed off-chain systems.

4.2 Consensus and network design

Consensus protocols allow participating nodes to agree on the valid state of the ledger. Proof of Work uses computational effort to help secure block production but can consume substantial energy. Proof of Stake uses economic stake and protocol rules to select or support validators, generally reducing the need for energy-intensive computation. Delegated or voting-based approaches can improve throughput by limiting the number of active validators, while practical Byzantine fault-tolerant protocols are commonly associated with permissioned settings in which participants are known. Each model makes different assumptions about trust, fault tolerance, performance, and governance; no single mechanism is optimal for every application (Singh, 2025; Saray & Kaplan, 2026).

4.3 Smart contracts

Smart contracts encode rules that can execute when specified conditions are met. They may automate settlement, permissions, workflow approvals, or the transfer of digital assets. Automation can be reduced by manual reconciliation to make the execution history auditable. However, a contract can execute a flawed rule exactly as programmed. Coding defects, inaccurate external inputs, ambiguous legal terms, and the difficulty of reversing an executed transaction make testing, independent auditing, controlled upgrades, and dispute procedures important. Code execution should not be mistaken for a complete substitute for legal agreements or institutional accountability.

4.4 Public, private, and consortium arrangements

Public networks allow broad participation and can offer open verification, but they may face throughput, fee, and confidentiality constraints. Private networks restrict participation to an organization or authorized group and can provide greater control over access and performance. Consortium models distribute governance among several institutions and may suit environments—such as healthcare networks or supply chains—in which multiple organizations need to coordinate while retaining some control over their own systems. The choice should follow the application's trust model, regulatory obligations, data sensitivity, and performance needs.

5. EVOLUTION AND RESEARCH DIRECTION

The literature describes a broad movement from cryptocurrency-centered systems toward

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 05 Sep-Oct; 2026 Page. No. 1114-1125

programmable applications and enterprise or cross-sector use. Bitcoin demonstrated a peer-to-peer transaction model; later programmable platforms made it possible to encode more complex business logic. Subsequent research has focused on scalability, interoperability, privacy, and integration with existing infrastructures (Mondal & Goswami, 2024; Singh, 2025). This trajectory is better understood as an expansion of possible uses than as a complete replacement of earlier generations.

The bibliometric study by López-Sorribes et al. (2023) analyzed 56,864 documents published from 2016 to 2022 across four major publishers. The reported annual total rose from 310 documents in 2016 to 19,305 in 2022. The authors also observed recurring research attention to security, smart contracts, applications, privacy, IoT, energy, and supply-related topics. These counts indicate growing publication activity in the databases and period studied; they should not be interpreted as direct measures of successful deployment or real-world impact. The study also suggests that blockchain increasingly appears as an enabling component within broader research fields, rather than always being the main subject.

6. APPLICATIONS ACROSS SECTORS

6.1 Finance and business processes

Blockchain-based systems can support peer-to-peer value transfer, tokenization, decentralized finance, and programmable settlement. Shared records may reduce reconciliation among institutions and provide traceable transaction histories. Nevertheless, price volatility in crypto-assets, uncertain regulatory treatment, cyber risks, transaction costs, and consumer-protection concerns can limit suitability. The existence of a blockchain does not by itself ensure that a financial product is sound, compliant, or fair.

6.2 Supply chains and logistics

Supply chains involve manufacturers, transport providers, distributors, retailers, regulators, and consumers, each of whom may maintain separate records. A shared ledger can record product origin, custody transfers, certifications, and selected events, while smart contracts may automate defined workflow steps. Such systems can strengthen provenance tracking and help detect inconsistencies or counterfeiting. Their effectiveness depends on the accuracy of the information entered, the participation of relevant actors, common data standards, and the reliability of links between physical goods and digital identifiers.

6.3 Healthcare and scientific information

Potential healthcare applications include access-permission management, audit trails for medical-record exchange, patient consent workflows, identity management, and pharmaceutical supply-chain tracking. A ledger may help institutions verify that a record or permission event has not been silently

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 05 Sep-Oct; 2026 Page. No. 1114-1125

altered. However, medical information is highly sensitive, and permanent or broadly replicated records may conflict with confidentiality and data-minimization requirements. In many cases, the safer architecture is to keep detailed health data in controlled repositories and use the ledger to record consent, access events, or integrity proofs. Interoperability with existing clinical systems and clear responsibility for correcting inaccurate records remain essential.

6.4 Education and public administration

Educational institutions can use verifiable credentials to simplify diploma and certificate checks and reduce reliance on repeated manual verification. Public agencies may explore auditable records for permits, registries, procurement, or expenditure tracking. These applications could improve traceability, but they cannot independently eliminate corruption, ensure fair decision-making, or guarantee that the original information was correct. Public-sector deployments also require accessibility, lawful data handling, transparent governance, and non-digital alternatives where needed.

6.5 Energy, IoT, and sustainability

Blockchain has been proposed for peer-to-peer energy trading, renewable-energy certificates, carbon-accounting records, and coordination among connected devices. IoT sensors can provide event data while a ledger record selected proofs or transactions. This combination may support traceability across organizations, but device security, data quality, latency, storage limits, and energy use must be addressed. High-frequency sensor data are generally unsuitable for direct, unrestricted storage on-chain; edge processing and off-chain storage may be more practical.

7. CROSS-CUTTING CHALLENGES

7.1 Scalability and cost

Some networks cannot process large transaction volumes at the speed or cost expected from conventional systems. Congestion can increase fees and delay confirmation. Layer-two systems, sharding, sidechains, and off-chain processing are among the approaches discussed in the literature, but they introduce their own security, coordination, and complexity considerations. Performance must be evaluated under realistic workloads rather than inferred from design claims alone.

7.2 Privacy and security

Cryptographic integrity does not remove vulnerabilities in applications, wallets, identity systems, bridges, smart contracts, or organizational procedures. Public visibility can also expose commercially or personally sensitive patterns. Privacy-preserving techniques, data minimization, access controls, secure key management, code audits, incident response, and independent testing should be part of system design from the outset.

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 05 Sep-Oct; 2026 Page. No. 1114-1125

7.3 Interoperability and data quality

Organizations often use different platforms, identifiers, data formats, and operating procedures. A blockchain that cannot exchange reliable information with existing databases or other ledgers may create another information silo instead of solving fragmentation. Interoperability requires technical interfaces as well as shared definitions, governance agreements, and procedures for handling inconsistent or disputed records. The quality of external data remains a fundamental limitation.

7 .4 Regulation, governance, and adoption

Legal requirements differ by jurisdiction and sector, while decentralized systems can make responsibility difficult to assign. Questions include who may change protocol rules, who is liable when a smart contract fails, how disputes are resolved, and how data-protection rights are respected. Adoption also requires skilled staff, user-friendly interfaces, organizational change, and integration with legacy systems. A technically functional prototype may therefore fail to become a sustainable service.

8. A PRACTICAL FRAMEWORK FOR RESPONSIBLE ADOPTION

Based on the themes across the reviewed sources, organizations should evaluate blockchain through a staged decision process:

1. Define the coordination problem. Identify the parties, the records they exchange, the sources of disagreement, and why a conventional shared database or trusted intermediary is insufficient.
2. Establish measurable outcomes. Specify indicators such as reconciliation time, verification cost, error rates, traceability, service availability, or user trust.
3. Select the governance model. Decide who can participate, validate transactions, access information, propose upgrades, and resolve disputes.
4. Minimize sensitive data. Keep personal and confidential information off-chain where feasible; use the ledger for proofs, permissions, and auditable events where appropriate.
5. Test security and performance. Assess throughput, latency, total cost, recovery procedures, key management, smart-contract correctness, and failure scenarios.
6. Plan integration and accountability. Define interfaces with existing systems, data standards, legal responsibilities, support arrangements, and procedures for correction or appeal.
7. Run a limited pilot and compare alternatives. Compare the blockchain design against a conventional database and evaluate results independently before scaling.

This framework emphasizes that adoption should be justified by the problem and the evidence. If one trusted organization can operate a reliable database and participants do not need independent verification, blockchain may add cost and complexity without proportional benefit. Contrarily, where several parties need a shared, auditable history and no single party is accepted as the sole authority, a carefully governed distributed ledger may be worth testing.

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 05 Sep-Oct; 2026 Page. No. 1114-1125

9. FUTURE RESEARCH AGENDA

First, future studies should compare the total cost and performance of blockchain and non-blockchain alternatives using common benchmarks and realistic workloads. Second, research should examine privacy-preserving data sharing and interoperable architectures that do not require sensitive information to be replicated across participants. Third, more empirical evaluation is needed in healthcare, public administration, supply chains, and energy systems, where operational benefits must be balanced against legal and ethical requirements. Fourth, the interaction of blockchain with AI and IoT deserves investigation, especially around data provenance, automated decisions, device security, and accountability. Finally, studies should measure organizational and social outcomes—not only transaction speed or technical security—including accessibility, trust, environmental impact, and the distribution of costs and benefits.

10. FUTURE PERSPECTIVES AND RESEARCH DIRECTIONS

Blockchain technology is increasingly recognized as a transformative digital infrastructure that is still in the process of maturation and expanding across multiple sectors. Current literature indicates that blockchain applications are no longer limited to financial systems but are progressively assuming strategic roles in healthcare, energy, supply chain management, smart infrastructures, and public services [59,60].

The cross-sectoral applications of blockchain technology, shared challenges, and emerging future directions are illustrated in Figure 2.

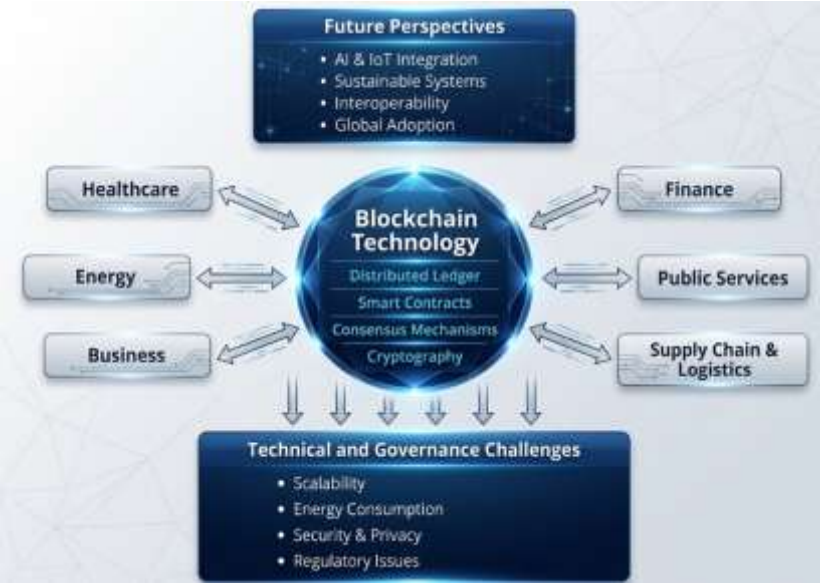


Figure 2. Framework Illustrating the Interconnections Among Core Components, Sectoral Applications, Technical Challenges, and Future Directions of Blockchain Technology.

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 05 Sep-Oct; 2026 Page. No. 1114-1125

Here is a breakdown of the key elements shown in the infographic:

❖ Central Core: Blockchain Pillars

At the center of the diagram is **Blockchain Technology**, which is built upon four fundamental technical pillars:

- **Distributed Ledger:** A shared, synchronized database spread across multiple nodes or locations, eliminating a single point of failure.
- **Smart Contracts:** Self-executing agreements stored on a blockchain that perform predefined tasks automatically when specified requirements are satisfied.
- **Consensus Mechanisms:** Protocols (like Proof of Work or Proof of Stake) that ensure all parties agree on the true state of the ledger.
- **Cryptography:** Advanced encryption techniques that secure transactions and guarantee data privacy and user anonymity.

❖ Connected Sectors: Industry Applications

The bi-directional arrows pointing outward show the primary sectors where blockchain is actively applied to improve efficiency, security, and traceability:

Industry Sector	Primary Use Case & Impact
Healthcare	Securing patient electronic health records (EHRs) and ensuring data privacy during sharing.
Energy	Enabling peer-to-peer (P2P) renewable energy trading networks and tracking carbon credits.
Business	Streamlining enterprise operations, digital identity management, and automated legal agreements.
Finance	Powering decentralized finance (DeFi), cross-border payments, and asset tokenization.
Public Services	Improving secure voting systems, land registry recording, and public record transparency.
Supply Chain & Logistics	Providing end-to-end tracking of goods to verify origin and prevent counterfeiting.

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 05 Sep-Oct; 2026 Page. No. 1114-1125

❖ **Future Perspectives (Top Layer)**

The top section highlights the evolutionary direction of technology as it matures towards global adoption:

- **AI & IoT Integration:** Combining blockchain with Artificial Intelligence and the Internet of Things to secure automated machine-to-machine transactions and data management.
- **Sustainable Systems:** Transitioning to green consensus models to minimize ecological impact.
- **Interoperability:** Developing cross-chain protocols so different blockchain networks can seamlessly communicate and transfer data.

❖ **Technical and Governance Challenges (Bottom Layer)**

The downward arrows point to the systemic obstacles that the industry must solve for widespread, mainstream implementation:

- **Scalability:** Increasing transaction processing speeds to match legacy payment systems (like Visa).
- **Energy Consumption:** Reducing the high electricity usage traditionally associated with mining networks.
- **Security & Privacy:** Defending against evolving cyber vulnerabilities while protecting user data.
- **Regulatory Issues:** Navigating complex international compliance laws and government oversight frameworks.

11. DISCUSSION

The reviewed literature converges on a central point: blockchain is a combination of technical and institutional arrangements. Distributed storage and cryptography can make records easier to verify, while consensus can coordinate participants who do not fully trust one another. Smart contracts can automate processes, and shared ledgers can support traceability across organizational boundaries. These advantages are conditional, however. They depend on correct data input, suitable governance, privacy-aware architecture, interoperability, and incentives for participants to maintain the system.

The field's evolution and the growth of related research show broad interest, but publication volume and the number of proposed use cases should not be confused with demonstrated effectiveness.

Stronger evidence will come from transparent pilots, longitudinal evaluations, comparisons with simpler alternatives, and explicit reporting of failures as well as benefits. A mature approach to blockchain therefore asks not only what the technology can do, but whether it is the most appropriate, proportionate, and accountable way to solve a defined problem.

12. CONCLUSION

Blockchain has expanded from its cryptocurrency origins into a potential infrastructure for shared verification, traceability, and programmable coordination. Its technical foundations—distributed ledgers, cryptographic integrity, consensus protocols, and smart contracts—can support applications across finance, supply chains, healthcare, education, public services, and energy. At the same time, scalability, privacy, security, interoperability, regulation, governance, and organizational readiness remain significant constraints. The most promising path is not universal deployment, but selective adoption grounded in clear requirements and measurable evidence. Responsible implementation should combine technical safeguards with data governance, legal clarity, user-centered design, and independent evaluation. Blockchain's long-term value will ultimately depend on whether it improves real processes in ways that justify its complexity and cost.

REFERENCES

1. López-Sorribes, S., Rius-Torrentó, J., & Solsona-Tehàs, F. (2023). A bibliometric review of the evolution of blockchain technologies. Sensors, 23(6), 3167. https://doi.org/10.3390/s23063167
2. Mondal, S., & Goswami, S. S. (2024). The evolution of blockchain technology: Applications, challenges, and future directions. Decision Making Advances, 2(1), 274–281. https://doi.org/10.31181/dma21202443
3. Saray, U., & Kaplan, Y. (2026). Blockchain technology: Applications, challenges, and future perspectives across multiple sectors. International Journal of New Findings in Engineering, Science and Technology, 4(2), 81–99. https://doi.org/10.61150/ijonfest.1900914
4. Singh, A. P. (2025). Blockchain technology: Core mechanisms, evolution, and future implementation challenges. arXiv preprint arXiv:2505.08772. https://arxiv.org/abs/2505.08772
5. Abdul, SSM. (2024). Navigating blockchain's twin challenges: Scalability and regulatory compliance. *Blockchains*, *2*(3), 265-298. https://doi.org/10.3390/blockchains2030013
8. Karaduman, Ö., & Gülhas, G. (2025). Blockchain-enabled supply chain management: A review of security, traceability, and data integrity amid the evolving systemic demand. *Applied Sciences*, *15*(9), 5168. https://doi.org/10.3390/app15095168
9. Çelik, S. E., & Özkır, V. (2021). Survey System Using Blockchain for Scientific Research. *Quantrade Journal of Complex Systems in Social Sciences, 3*(2), 45-67. https://izlik.org/JA35CH88WT

10. Kaya, İ., & Demir, S. (2021). Health 4.0: Blockchain Applications in Healthcare. *Journal of Investigations on Engineering and Technology*, *4*(2), 69-76. https://izlik.org/JA88NE66KJ
11. Shaikh, M., Memon, SA, Ebrahimi, A., & Wiil, UK. (2025). A systematic literature review for blockchain-based healthcare implementations. *Healthcare*, *13*(9), 1087. https://doi.org/10.3390/healthcare13091087
12. Khan, AA., Baqasah, AM., Alsafyani, MA., Alsufyani, H., Alhazmi. A., & Ullah, S. (2026). Blockchain for e-healthcare: A review on secure data management frameworks and future challenges. *Journal of Big Data*, *13*(20). https://doi.org/10.1186/s40537-025-01348-7
13. Singh, J., Bharany, S., Rani, S., Rehman, AU., Taye, BM., Pant, R., & Kaur, U. (2025). A systematic review of blockchain, AI, and cloud integration for secure digital ecosystems. *International Journal of Networked and Distributed Computing*, *13*(28). https://doi.org/10.1007/s44227-025-00072-1
14. Sabiri, K., Sousa, F., & Rocha, T. (2025). A systematic review of privacy-preserving blockchain applications in healthcare. *Multimedia Tools and Applications, 84*, 39925-39980. https://doi.org/10.1007/s11042-024-20541-z
15. Sivasankari, B., & Varalakshmi, P. (2022). Blockchain and IoT technology in healthcare: A review. *Studies in Health Technology and Informatics*, *294*, 277-278. https://doi.org/10.3233/SHTI220455
16. Liu, X., Dong, F., Shui, W. & Geng G. (2025). Blockchain in digital cultural heritage resources: Technological integration, consensus mechanisms, and future directions. *npj Heritage Science*, *13*, 235. https://doi.org/10.1038/s40494-025-01818-4
17. Tagde, P., Tagde, S., Bhattacharya, T., Islam, S., Rahman, MH., Kaushik, S. (2021). Blockchain and artificial intelligence technology in e-health.*Environmental Science and Pollution Research*, *28*, 52810-52831. https://doi.org/10.1007/s11356-021-16223-0
18. Wu, J., Bian. Z., Gao, H. & Wang, Y. (2025). A blockchain-based secure data transaction and privacy preservation scheme in iot system. *Sensors*, *25*(15), 4854. https://doi.org/10.3390/s25154854