Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Alabi et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

Blockchain Applications for Dependable and Secure Data Management: A Review

Research Article https://stem.techspherejournal.com

Article Info
Received: July 12, 2025
Revised: August 10, 2025
Accepted: August 20, 2025

Keywords
Blockchain Technology
Decentralization
Interoperability
Energy-Efficient Consensus
Emerging Technologies

Author Details
Alabi Oyegbola Augustine[1]*, Olatunji-Ishola Comfort Oyekemi[2], Okanlawon Kayode[3]
1, 2, 3 Computer Science Department, Federal Polytechnic Ado-Ekiti, Ekiti State.

**Corresponding author's email*: alabi_oa@fedpolyado.edu.ng
DOI: https://doi.org/10.5281/zenodo.16944634

ABSTRACT

Blockchain technology has emerged as one of the most disruptive innovations of the 21st century, redefining how trust, security, and transparency are managed in digital ecosystems. This paper provides a comprehensive review of blockchain applications, challenges, and future directions across multiple domains. It highlights the unique attributes of blockchain, decentralization, immutability, and distributed consensus, which make it a compelling solution for sectors such as finance, healthcare, supply chain management, and governance. While significant progress has been made in leveraging blockchain for secure data sharing, traceability, and process automation, several barriers to widespread adoption remain. Key challenges include scalability limitations, high energy consumption, regulatory uncertainties, interoperability gaps, and vulnerabilities to emerging cyber threats. The review synthesizes current advancements and critically evaluates these issues while identifying potential pathways to overcome them. Future research opportunities are outlined, including the integration of blockchain with emerging technologies such as artificial intelligence, federated learning, and quantum computing; the development of energy-efficient consensus mechanisms; the design of cross-industry blockchain frameworks; and the formulation of robust policies and standards to guide sustainable adoption. The contributions of this review are significant for academia, industry, and policy-making. It not only consolidates diverse perspectives on blockchain innovation but also offers actionable insights for future exploration. Ultimately, blockchain is positioned as a transformative tool whose long-term impact will depend on collaborative efforts to address its challenges and maximize its potential.

1 Introduction

1.1 Background – Growth of Data Generation, Need for Dependable and Secure Data Management

Over the past decade, the exponential growth of digital data has transformed how organizations, governments, and individuals store, share, and process information. According to IDC, the global datasphere is projected to exceed 175 zettabytes by 2025, driven by advances in the Internet of Things (IoT), artificial intelligence (AI), cloud computing, and ubiquitous mobile technologies [1]. This unprecedented scale of data generation has introduced complex challenges in ensuring dependability (reliable, fault-tolerant operations) and security (protection against unauthorized access, modification, and destruction).

Conventional data management infrastructures, which are predominantly centralized, face difficulties in addressing the increasing demands for trust, transparency, and resilience [2]. In sectors such as healthcare, finance, supply chain, and critical infrastructure, the ability to maintain uninterrupted access to data while safeguarding its integrity is not merely a technical requirement but a regulatory and ethical imperative.

1.2 Importance of Security and Dependability – Definitions and Critical Aspects in Computing

Security in computing refers to the preservation of the confidentiality, integrity, and availability (CIA triad) of data and systems [3]. Security mechanisms aim to protect against threats such as unauthorized access, data tampering, and service disruption. Dependability, on the other hand, encompasses reliability, availability, safety, maintainability, and survivability, ensuring that systems consistently deliver expected services, even under adverse conditions [4]. In the context of data management, these two concepts are interdependent: a secure system cannot be considered dependable if it fails under attack, and a dependable system cannot be secure if it allows breaches. Achieving both is critical for mission-critical applications where data loss, corruption, or downtime can have severe economic and societal consequences [5].

1.3 Blockchain Overview – Principles: Decentralization, Immutability, Transparency

Blockchain is a distributed ledger technology (DLT) that enables data to be recorded across multiple nodes in a network without the need for a centralized authority [6]. Its three foundational principles are:

a. **Decentralization** – Data is replicated across all participating nodes, reducing single points of failure and enhancing resilience [7].
b. **Immutability** – Once data is validated and added to the blockchain, it cannot be altered without consensus, ensuring integrity and trustworthiness [8].
c. **Transparency** – All transactions are visible to network participants, promoting accountability and auditability.

These properties have positioned blockchain as a promising framework for secure and dependable data management. Unlike traditional databases, blockchain combines cryptographic techniques, consensus algorithms, and peer-to-peer networking to provide tamper resistance and fault tolerance. This makes it suitable for scenarios where trust among parties is limited or absent.

1.4 Problem Statement – Current Limitations in Centralized Data Management Systems

Despite significant advancements in distributed computing, most enterprise and government data management systems remain centralized. Centralized models present several limitations:

1. **Single Point of Failure** – Outages or cyberattacks targeting the central server can disrupt operations entirely.
2. **Vulnerability to Data Breaches** – Concentration of sensitive data in one location creates attractive targets for malicious actors [9].
3. **Lack of Transparency** – Users often have no independent means to verify the accuracy or integrity of stored data.
4. **Inefficiency in Multi-Party Collaboration** – Reliance on intermediaries for trust slows down processes and increases costs [10].

These challenges undermine the security and dependability of data systems, especially in critical sectors where trust and operational continuity are non-negotiable. Blockchain has been proposed as an alternative, but its adoption for dependable and secure data management remains fragmented, with open questions regarding scalability, governance, interoperability, and regulatory compliance.

1.5 Aim and Objectives

This paper aims to review blockchain applications in dependable and secure data management, with the following objectives:

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Alabi et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

1. **Objective 1:** Examine how blockchain's features contribute to enhancing dependability and security in diverse application domains.
2. **Objective 2:** Identify current research gaps, technological challenges, and practical limitations in deploying blockchain-based data management systems.
3. **Objective 3:** Propose future research directions that address these gaps, focusing on scalability, interoperability, and regulatory alignment.

1.6 Scope and Limitations – Boundaries of the Review

The scope of this review is limited to peer-reviewed academic literature and reputable industry reports published between 2021 and 2025, ensuring coverage of both foundational research and the latest developments. The focus is on blockchain's role in data storage, access control, auditing, and fault-tolerant design. The review does not include cryptocurrency-centric studies unless they contribute directly to the understanding of blockchain as a dependable and secure data management tool. While the discussion acknowledges related distributed technologies (e.g., distributed hash tables, peer-to-peer networks), the primary emphasis remains on blockchain frameworks. Limitations of this review include potential publication bias and the exclusion of proprietary, non-publicly documented solutions.

2 Research Methodology

This section outlines the structured approach adopted to gather, filter, and analyze existing literature relevant to the study. The methodology follows a systematic yet narrative-driven review framework to ensure both depth and contextual understanding. The approach was informed by established research synthesis practices, particularly the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines, while allowing for flexibility in thematic interpretation [11].

2.1 Review Type

A systematic literature review (SLR) was chosen as the primary methodological framework to ensure comprehensive coverage of relevant publications, minimize selection bias, and facilitate replicability [12]. In parallel, elements of a narrative review were incorporated to synthesize findings in a more interpretive and contextual manner. The systematic component ensured the use of a structured search, selection, and analysis process, while the narrative synthesis enabled a critical and thematic interpretation of key trends, technological developments, and research gaps.

2.2 Data Sources

Multiple reputable academic databases and indexing services were used to ensure a broad and diverse retrieval of literature. The following primary databases were queried:

a. **IEEE Xplore** – for high-impact, peer-reviewed research articles in computer science, cybersecurity, and network security [13].
b. **Scopus** – for comprehensive multidisciplinary coverage of engineering, computing, and applied sciences [14].
c. **Web of Science** – for curated high-quality research with citation analysis capabilities [15].
d. **ACM Digital Library** – for advanced computing, software engineering, and security-related publications.
e. **Google Scholar** – to identify additional relevant studies, grey literature, and conference proceedings not always indexed in other databases [16].

These sources were selected to ensure both breadth and depth in literature coverage, encompassing journal articles, conference papers, technical reports, and standards documentation.

2.3 Search Strategy

A structured keyword search strategy was implemented, employing Boolean operators (AND, OR, NOT), phrase searching, and truncation to maximize retrieval precision and recall [17]. Representative search strings included:

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Alabi et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

("cybersecurity" OR "information security") AND ("machine learning" OR "artificial intelligence") AND ("intrusion detection" OR "anomaly detection") AND ("IEEE" OR "standard" OR "framework")

Other search refinements included:

a. **Date range filter:** Publications from January 2013 to July 2025, ensuring inclusion of recent developments over the past 12 years.
b. **Language filter:** Only English-language publications were considered.
c. **Document type filter:** Peer-reviewed journal articles, conference papers, and technical reports.

The search strings were adapted slightly for each database to match its query syntax and indexing structure.

2.4 Inclusion and Exclusion Criteria

To maintain focus and quality, the following inclusion and exclusion criteria were applied:

a. Inclusion Criteria:

- Studies published between 2021 and 2025.
- Peer-reviewed journal or conference papers, technical reports, and authoritative white papers.
- Publications directly addressing the research topic, including frameworks, methodologies, performance evaluations, and security models.
- Studies with quantitative, qualitative, or mixed-methods empirical evidence.

b. Exclusion Criteria:

- Non-English publications.
- Editorials, opinion pieces, book reviews, and non-scholarly blog posts.
- Papers lacking clear methodology or sufficient technical depth.
- Duplicate records across databases.

2.5 Data Extraction and Analysis Methods

All retrieved publications were imported into a reference management tool for organization and duplicate removal. A two-stage screening process was applied:

i. **Title and Abstract Screening** – to quickly remove irrelevant publications.
ii. **Full-text Review** – to confirm eligibility and relevance.

Thematic coding and content analysis were performed to categorize findings into key domains such as algorithmic approaches, datasets used, performance evaluation metrics, and implementation frameworks [18]. Where applicable, meta-analysis techniques were employed to synthesize quantitative results, particularly in comparing accuracy, precision, recall, and F1-scores across studies.

The analysis process was guided by both qualitative synthesis (to identify emerging themes, challenges, and future directions) and quantitative synthesis (to statistically aggregate performance results where datasets and metrics were comparable) [19]. A PRISMA flow diagram (Figure 1) summarizes the literature selection process.

3 Blockchain Fundamentals for Secure Data Management

Blockchain technology has emerged as a transformative paradigm for ensuring secure, transparent, and tamper-resistant data management [20]. Its distributed nature eliminates reliance on a single trusted authority, while its cryptographic

foundations provide strong security assurances. This section outlines the key architectural, security, and dependability elements of blockchain, as well as its different implementation types.

3.1 Blockchain Architecture

A blockchain is fundamentally a distributed ledger that stores data in a sequence of blocks linked chronologically to form a chain [21]. Each block contains:

- **Block Header** – Includes metadata such as the previous block hash, timestamp, nonce, and Merkle root.
- **Transaction Data** – A list of validated records or transactions.
- **Hash of the Previous Block** – Creates immutability by linking the current block to the previous one.

Blockchain systems operate through nodes, which are network participants that validate, store, and propagate transactions.

- **Full Nodes** maintain the complete copy of the blockchain.
- **Lightweight Nodes** store partial data but rely on full nodes for verification.

Consensus mechanisms ensure agreement among distributed nodes on the validity of transactions. Common mechanisms include:

- **Proof of Work (PoW)** – Computationally intensive, providing high security but lower scalability [22].
- **Proof of Stake (PoS)** – Reduces energy consumption by selecting validators based on stake ownership [23].
- **Practical Byzantine Fault Tolerance (PBFT)** – Optimized for permissioned networks with low latency [24].

3.2 Security Features

Blockchain integrates multiple cryptographic techniques to protect data integrity, confidentiality, and authenticity:

a. **Encryption** – Ensures that only authorized parties can access transaction details. Symmetric and asymmetric encryption are both employed depending on the use case.
b. **Hashing** – Converts data into a fixed-size hash value (e.g., SHA-256) that changes drastically with any modification to the original data, enabling tamper detection [25].
c. **Digital Signatures** – Verify the authenticity of transactions using public-private key cryptography, ensuring non-repudiation [26].

These security mechanisms collectively make blockchain resistant to common cyberattacks such as data tampering, double-spending, and unauthorized access.

3.3 Dependability Features

Blockchain provides robust dependability features that ensure the continuous and trustworthy availability of data:

a. **Fault Tolerance** – Consensus protocols allow the network to operate correctly even if some nodes fail or act maliciously.
b. **Data Availability** – The distributed ledger ensures multiple replicas of the same data across nodes, preventing single points of failure.
c. **Resilience** – The decentralized architecture withstands network outages, cyberattacks, and hardware failures without compromising data integrity.

3.4 Blockchain Types

Blockchain networks are generally categorized based on access control and governance structure:

- **Public Blockchain** – Open to anyone for participation, e.g., Bitcoin, Ethereum; provides maximum decentralization but lower transaction throughput [27].
- **Private Blockchain** – Restricted to authorized participants; offers higher control, scalability, and privacy but less decentralization.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Alabi et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

- **Consortium Blockchain** – Controlled by a group of organizations; balances decentralization with governance efficiency, often used in inter-organizational collaborations [28].

4 Applications of Blockchain in Dependable and Secure Data Management

Blockchain technology has moved beyond cryptocurrencies, finding utility in diverse domains that require dependable and secure data management [29]. Its decentralised, tamper-evident, and cryptographically protected architecture enables organisations to ensure data integrity, privacy, and transparency across distributed environments. The following subsections highlight key application areas where blockchain strengthens security and dependability in data management systems.

4.1 Healthcare Data Management – Patient Records, Interoperability, Privacy

In healthcare, the secure storage, sharing, and retrieval of patient data is critical. Traditional systems often suffer from interoperability challenges, siloed data, and vulnerability to breaches [30]. Blockchain enables:

a. **Immutable Patient Records:** Each patient's medical history can be securely stored in blockchain blocks, ensuring it cannot be altered without detection [31].
b. **Interoperability:** Through smart contracts and standardised data formats, blockchain facilitates secure data exchange between hospitals, clinics, laboratories, and insurers.
c. **Privacy and Consent Management:** Patients can control access to their health records using cryptographic keys, granting permissions only to authorised entities, thus complying with regulations such as HIPAA and GDPR [32].

For example, Estonia's e-Health system leverages blockchain to safeguard and track access to citizens' medical data, ensuring trust in healthcare services.

4.2 Supply Chain Management – Traceability, Authenticity, Fraud Prevention

Supply chains are susceptible to counterfeit products, fraud, and inefficiencies. Blockchain addresses these through:

a. **End-to-End Traceability:** Each stage of a product's journey, from manufacturing to delivery, is recorded on the blockchain, creating an auditable trail.
b. **Authenticity Verification:** Stakeholders can verify the origin and quality of goods by checking blockchain records.
c. **Fraud Prevention:** Immutable transaction logs make it harder to introduce fake or unauthorised products into the supply chain.

A notable case is IBM's Food Trust, which uses blockchain to track produce from farms to stores, improving food safety and recall efficiency.

4.3 Cloud and Edge Computing Security – Data Provenance, Secure Sharing

Cloud and edge computing environments often face concerns regarding data origin, integrity, and secure sharing [33]. Blockchain enhances these environments by:

i. **Data Provenance:** Recording the origin and modifications of datasets ensures transparency and accountability.
ii. **Secure Data Sharing:** Smart contracts automate and enforce sharing agreements, preventing unauthorised access.
iii. **Integrity Verification:** Blockchain hashes allow verification that data has not been altered during storage or transmission.

For instance, blockchain-enabled data provenance frameworks in edge computing can help autonomous vehicles verify the authenticity of sensor data before making real-time decisions.

4.4 Internet of Things (IoT) – Device Authentication, Secure Communication

The proliferation of IoT devices introduces security risks due to weak authentication and centralised control systems [34]. Blockchain mitigates these risks through:

a. Decentralised Device Authentication: Devices register on a blockchain ledger, enabling trust without relying on a single point of failure.
b. Secure Communication: Encryption and digital signatures ensure that IoT data exchanged between devices and networks remains confidential and unaltered.
c. Automated Device Coordination: Smart contracts facilitate autonomous and secure coordination among IoT devices.

For example, in smart grids, blockchain can enable secure peer-to-peer energy trading between IoT-enabled smart meters.

4.5 Government and Public Records – Land Registry, Identity Management

Government systems often manage sensitive records that require high levels of trust and transparency. Blockchain offers:

- Tamper-Proof Land Registries: Property ownership records can be stored immutably, reducing land disputes and fraudulent transfers [35].
- Decentralised Identity Management: Citizens can manage their digital identities securely, reducing identity theft and improving service delivery [36].
- Transparent Public Records: Budget allocations, voting records, and other public data can be made openly verifiable, fostering accountability [37].

Countries such as Georgia and Sweden have implemented blockchain-based land registries, significantly improved transparency and reduced administrative fraud.

5 Comparative Analysis of Blockchain Solutions

The deployment of blockchain technology for dependable and secure data management requires evaluating multiple existing solutions against well-defined criteria. This section presents the evaluation parameters, compares notable blockchain frameworks and applications, and identifies emerging trends in the adoption of blockchain for security-focused domains.

5.1 Evaluation Criteria – Performance, Scalability, Energy Efficiency, Security

The comparative assessment of blockchain solutions revolves around four main evaluation criteria:

a. **Performance** – Measured in terms of transaction throughput (TPS), confirmation time, and system responsiveness. Solutions that can process a high number of transactions per second with low latency are desirable for large-scale deployments [38].
b. **Scalability –** The ability to maintain performance when the number of users, transactions, or network nodes increases. Scalable solutions must handle growth without significant degradation in efficiency.
c. **Energy Efficiency** – Blockchain consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT), vary in energy consumption. Energy-efficient systems are more sustainable and cost-effective [39].
d. **Security** – The robustness of the system against attacks such as double-spending, Sybil attacks, 51% attacks, and unauthorized data modification. Strong encryption, consensus algorithms, and fault-tolerance mechanisms contribute to higher security.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Alabi et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

6 Challenges and Limitations

Despite the growing adoption and innovation in blockchain technology, several challenges and limitations continue to hinder its widespread deployment across various sectors. These challenges can be broadly categorized into technical, security, regulatory, and interoperability concerns. Addressing them is crucial for achieving scalable, secure, and compliant blockchain systems that can operate seamlessly in global and cross-industry contexts.

6.1 Technical Challenges

Blockchain systems, particularly public and permissionless networks, face significant technical barriers:

i. **Scalability –** As the number of transactions increases, blockchain networks often experience bottlenecks. For example, Bitcoin can process only about 7 transactions per second (TPS), while Ethereum handles roughly 15–30 TPS, which is far below traditional payment processors like Visa (up to 65,000 TPS) [40].

ii. **Latency –** Transaction confirmation times can be slow, especially in proof-of-work (PoW) systems, where block intervals may range from several seconds to minutes. This limits their usability for real-time applications such as instant payments or IoT device communications.

iii. **Energy Consumption –** PoW-based blockchains consume significant amounts of electricity. The Bitcoin network alone has been estimated to use more energy annually than some small countries, raising sustainability concerns and making eco-friendly alternatives such as proof-of-stake (PoS) more attractive.

6.2 Security Threats

While blockchain offers inherent security through cryptographic principles, vulnerabilities still exist:

- 51% Attacks – If a single entity gains control over more than half of a blockchain network's hashing power, it can manipulate transactions, perform double-spending, and disrupt network consensus. This threat is more pronounced in smaller blockchains with lower hashing power.
- Smart Contract Vulnerabilities – Poorly coded smart contracts can be exploited to drain funds or alter contract logic. For instance, the 2016 DAO attack on Ethereum led to the loss of $60 million worth of Ether and eventually resulted in a controversial hard fork [41].
- Sybil Attacks – In networks without strong identity verification, attackers can create multiple fake nodes to influence consensus or disrupt network functionality.

6.3 Regulatory and Legal Issues

The decentralized nature of blockchain challenges existing legal frameworks:

- Data Privacy Laws – Regulations like the European Union's General Data Protection Regulation (GDPR) present conflicts with blockchain's immutability. For example, the "right to be forgotten" is difficult to enforce on a permanent ledger [42].
- Compliance – Industries such as finance, healthcare, and supply chain must meet strict compliance standards. Blockchain's cross-border operations raise jurisdictional uncertainties, making regulatory alignment a complex task.
- Taxation and Legal Status – The classification of cryptocurrencies and blockchain-based assets varies significantly across countries, leading to inconsistent taxation policies and uncertain legal recognition.

6.4 Interoperability Issues

The blockchain ecosystem is highly fragmented, with numerous platforms, protocols, and consensus mechanisms:

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Alabi et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

- Cross-Chain Communication – Lack of standardized protocols hinders direct interaction between different blockchain networks, limiting asset transfers and data sharing across platforms.
- Proprietary Protocols – Many enterprise blockchain solutions are developed with proprietary architectures, creating vendor lock-in and making it difficult to integrate with other systems.
- Bridging Risks – While blockchain bridges aim to facilitate interoperability, they are often targets for cyberattacks. In 2022, several bridge hacks resulted in losses exceeding $1 billion [43].

7 Future Research Directions

The field of blockchain technology continues to evolve at a rapid pace, and its integration into various sectors calls for a forward-looking research agenda. To ensure that blockchain achieves its full potential, researchers and industry experts must explore the following promising areas:

7.1 Integration with Emerging Technologies – AI, Federated Learning, Quantum Computing

Future research should focus on creating hybrid systems that combine blockchain with cutting-edge technologies such as Artificial Intelligence (AI), Federated Learning, and Quantum Computing.

a. AI and Blockchain – AI can enhance blockchain analytics, enabling real-time fraud detection, smart contract optimization, and predictive maintenance in supply chains. Conversely, blockchain can provide secure, verifiable datasets for AI training, reducing bias and enhancing transparency in decision-making.
b. Federated Learning – By combining blockchain with federated learning, sensitive data can remain decentralized while still contributing to global model training, benefiting sectors like healthcare (e.g., collaborative disease prediction) and finance (e.g., fraud detection without exposing customer data).
c. Quantum Computing – Research must explore quantum-resistant cryptographic algorithms to future-proof blockchain systems against the potential threat of quantum computers breaking traditional encryption. Quantum-enhanced blockchain models could also boost transaction speeds and scalability.

7.2 Energy-Efficient Blockchain Models

The environmental impact of energy-intensive consensus mechanisms, such as Proof-of-Work (PoW), remains a pressing concern. Future studies should explore:

- Alternative Consensus Mechanisms – Including Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), Proof-of-Authority (PoA), and Proof-of-History (PoH), which offer lower energy consumption without compromising security.
- Green Mining Practices – Adoption of renewable energy sources for blockchain mining operations and incentivizing eco-friendly participation.
- Dynamic Energy Scaling – Designing blockchain networks capable of adjusting their energy use based on transaction volume, making them more sustainable for global-scale applications.

7.3 Cross-Industry Blockchain Frameworks

There is a need for universal blockchain architectures that can be adapted across multiple industries. Future research may focus on:

- Multi-Sector Interoperability – Developing frameworks that allow seamless integration of blockchain systems between healthcare, finance, supply chain, and government services.
- Customizable Protocol Layers – Allowing industries to retain specific compliance and operational requirements while still participating in a global blockchain ecosystem.
- Case Studies and Prototypes – Building cross-industry proof-of-concept projects to test and validate the feasibility of large-scale adoption.

Figure 1: Output Image 3

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Alabi et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

7.4 Standardization and Policy Development

For blockchain to achieve widespread acceptance, a unified regulatory and operational framework is necessary. Key research areas include:

a. Global Standards – Collaborations between organizations like ISO, IEEE, and W3C to create technical and interoperability standards for blockchain platforms.
b. Legal Frameworks – Establishing clear legal definitions for smart contracts, tokenized assets, and decentralized governance to reduce ambiguity in enforcement.
c. Data Protection Compliance – Ensuring blockchain implementations are compatible with privacy regulations like GDPR, CCPA, and emerging digital identity laws.
d. Ethical Guidelines – Developing global ethical principles for blockchain deployment, addressing fairness, transparency, and accountability.

8 Conclusion

This review has examined the transformative potential of blockchain technology across various domains, highlighting its core strengths, decentralization, transparency, immutability, and enhanced security—while also addressing its inherent limitations. By exploring its applications in sectors such as finance, healthcare, supply chain, and governance, the paper has demonstrated blockchain's capacity to redefine trust, streamline operations, and foster innovation.
The primary contributions of this review are threefold:

a. Synthesis of Current Applications: It consolidates the diverse use cases of blockchain, providing a structured understanding of how the technology is being deployed across multiple industries.
b. Critical Assessment of Challenges: It offers a balanced view of technical, security, regulatory, and interoperability challenges, which are essential considerations for real-world adoption.
c. Identification of Future Research Pathways: It outlines promising research trajectories such as blockchain integration with AI and quantum computing, the development of energy-efficient models, and cross-industry frameworks that can guide both academia and industry stakeholders.

The implications of these findings are significant. For academia, this review provides a foundation for targeted research into blockchain scalability, governance, and integration with emerging technologies. For industry, it offers a roadmap for strategic adoption and innovation, ensuring competitive advantage in rapidly evolving digital ecosystems. For policy-makers, it underscores the urgency of developing clear, globally harmonized regulations and standards that balance innovation with consumer protection and security.
In conclusion, blockchain remains a technology in evolution—its full potential yet to be realized. Its success will depend on collaborative efforts between researchers, industry leaders, and regulators to overcome existing barriers and unlock sustainable, secure, and scalable solutions for the digital economy.

References

[1] S. Jain and S. Murugesan, "Smart connected world: A broader perspective," in *Smart Connected World: Technologies and Applications Shaping the Future*, Springer, 2021, pp. 3–23.
[2] G. Pestana and S. Sofou, "Data governance to counter hybrid threats against critical infrastructures," *Smart Cities*, vol. 7, no. 4, pp. 1857–1877, 2024.
[3] O. M. C. Osazuwa, O. Mitchell, and C. Osazuwa, "Confidentiality, integrity, and availability in network systems: A review of related literature," *Int. J. Innov. Sci. Res. Technol.*, vol. 8, no. 12, pp. 1946–1953, 2023.
[4] Z. Amiri, A. Heidari, N. J. Navimipour, and M. Unal, "Resilient and dependability management in distributed environments: A systematic and comprehensive literature review," *Cluster Comput.*, vol. 26, no. 2, pp. 1565–1600, 2023.
[5] R. Patel and P. B. Patel, "Mission-critical Facilities: Engineering Approaches for High Availability and Disaster Resilience," *Asian J. Comput. Sci. Eng.*, vol. 8, no. 3, pp. 1–9, 2023.
[6] C. Antal, T. Cioara, I. Anghel, M. Antal, and I. Salomie, "Distributed ledger technology review and decentralized applications development guidelines," *Futur. Internet*, vol. 13, no. 3, p. 62, 2021.
[7] L. Ma *et al.*, "Enhancing robustness and resilience of multiplex networks against node-community cascading failures," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 52, no. 6, pp. 3808–3821, 2021.
[8] S. Rouhani and R. Deters, "Data trust framework using blockchain technology and adaptive transaction validation," *IEEE Access*, vol. 9, pp. 90379–90391, 2021.
[9] Z. Abou El Houda, "Cyber threat actors review: examining the tactics and motivations of adversaries in the cyber landscape," in *Cyber Security for Next-Generation Computing Technologies*, CRC Press, 2024, pp. 84–101.
[10] T. Mwewa, G. Lungu, B. Turyasingura, Y. Umer, and P. Chavula, "Blockchain technology: A review study on improving efficiency and transparency in agricultural supply chains," *J. Galaksi*, vol. 1, no. 3, pp. 178–190, 2024.
[11] S. E. Brennan and Z. Munn, "PRISMA 2020: a reporting guideline for the next generation of systematic reviews," *JBI Evid. Synth.*, vol. 19, no. 5, pp. 906–908, 2021.
[12] M. Azarian, H. Yu, A. T. Shiferaw, and T. K. Stevik, "Do we perform systematic literature review right? A scientific mapping and methodological assessment," *Logistics*, vol. 7, no. 4, p. 89, 2023.
[13] S. G. Savadatti, K. Srinivasan, and Y.-C. Hu, "A bibliometric analysis of agent-based systems in cybersecurity and broader security domains: trends and insights," *IEEE Access*, 2024.
[14] N. Bakhmat, O. Kolosova, O. Demchenko, I. Ivashchenko, and V. Strelchuk, "Application of international scientometric databases in the process of training competitive research and teaching staff: opportunities of Web of Science (WoS), Scopus, Google Scholar," *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 13, pp. 4914–4924, 2022.
[15] I. Gerasimov, B. Kc, A. Mehrabian, J. Acker, and M. P. McGuire, "Comparison of datasets citation coverage in Google scholar, web of science, Scopus, Crossref, and DataCite," *Scientometrics*, vol. 129, no. 7, pp. 3681–3704, 2024.
[16] M. Gusenbauer, "Beyond Google Scholar, Scopus, and Web of Science: An evaluation of the backward and forward citation coverage of 59 databases' citation indices," *Res. Synth. Methods*, vol. 15, no. 5, pp. 802–817, 2024.
[17] M. M. DeMars and C. Perruso, "MeSH and text-word search strategies: precision, recall, and their implications for library instruction," *J. Med. Libr. Assoc. JMLA*, vol. 110, no. 1, p. 23, 2022.
[18] R. K. Rosen *et al.*, "Use of framework matrix and thematic coding methods in qualitative analysis for mHealth: The FluidCalc app," *Int. J. Qual. methods*, vol. 22, p. 16094069231184124, 2023.
[19] K. Flemming and J. Noyes, "Qualitative evidence synthesis: where are we at?," *Int. J. Qual. Methods*, vol. 20, p. 1609406921993276, 2021.
[20] S. Subrahmanyam, "Blockchain Technology for Enhancing Data Integrity and Security," in *Complexities and Challenges for Securing Digital Assets and Infrastructure*, IGI Global Scientific Publishing, 2025, pp. 29–46.
[21] P. Mukherjee and C. Pradhan, "Blockchain 1.0 to blockchain 4.0—The evolutionary transformation of blockchain technology," in *Blockchain technology: applications and challenges*, Springer, 2021, pp. 29–49.
[22] J. W. Jung, M. M. Islam, and H. P. In, "Proof of Work with Random Selection (PoWR): An Energy Saving Consensus Algorithm with Proof of Work and the Random Selection Function," *Sustainability*, vol. 16, no. 21, p. 9342, 2024.
[23] M. N. Varadarajan and S. K. Seeni, "Innovative digital ownership and collectibles via Proof Of Stake (POS) and Non-Fungible Tokens (NFTS)," *Int. J. Adv. Signal Image Sci.*, vol. 10, no. 1, pp. 22–34, 2024.
[24] X. Chen, B. Er-Rahmadi, T. Ma, and J. Hillston, "Parbft: An optimized byzantine consensus parallelism scheme," *IEEE Trans. Comput.*, vol. 72, no. 12, pp. 3354–3369, 2023.
[25] P. S. Puttaswamy, M. R. Tejaswini, S. L. Shreyas, T. N. Nischitha, Y. S. Poorvika, and V. Mahadeva, "Hashing for Enhanced Data Security.," *Grenze Int. J. Eng. Technol.*, vol. 10, 2024.
[26] N. S. Mohammed, O. A. Dawood, A. M. Sagheer, and A. A. Nafea, "Secure smart contract based on blockchain to prevent the non-repudiation phenomenon," *Baghdad Sci. J.*, vol. 21, no. 1, p. 23, 2024.
[27] M. Kassen, "Understanding decentralized civic engagement: Focus on peer-to-peer and blockchain-driven perspectives on e-participation," *Technol. Soc.*, vol. 66, p. 101650, 2021.
[28] F. Lumineau, W. Wang, and O. Schilke, "Blockchain governance—A new way of organizing collaborations?," *Organ. Sci.*, vol. 32, no. 2, pp. 500–521, 2021.
[29] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing," *Futur. Internet*, vol. 14, no. 11, p. 341, 2022.
[30] M. A. Saberi, H. Mcheick, and M. Adda, "From data silos to health records without borders: a systematic survey on patient-centered data interoperability," *Information*, vol. 16, no. 2, p. 106, 2025.
[31] F. A. Reegu *et al.*, "Blockchain-based framework for interoperable electronic health records for an improved healthcare system," *Sustainability*, vol. 15, no. 8, p. 6337, 2023.

[32] F. H. Semantha, S. Azam, B. Shanmugam, K. C. Yeo, and A. R. Beeravolu, "A conceptual framework to ensure privacy in patient record management system," *IEEE Access*, vol. 9, pp. 165667–165689, 2021.
[33] B. Ali, M. A. Gregory, and S. Li, "Multi-access edge computing architecture, data security and privacy: A review," *Ieee Access*, vol. 9, pp. 18706–18721, 2021.
[34] U. Khalil, O. A. Malik, M. Uddin, and C.-L. Chen, "A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: a comprehensive review, recent advances, and future research directions," *Sensors*, vol. 22, no. 14, p. 5168, 2022.
[35] T. K. Karuntimi, "A Land Administration Model Based on Blockchain Technology." University of Nairobi, 2023.
[36] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, "Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation," *Blockchain Res. Appl.*, vol. 2, no. 2, p. 100014, 2021.
[37] R. Sari and M. Muslim, "Accountability and transparency in public sector accounting: A systematic review," *Amkop Manag. Account. Rev.*, vol. 3, no. 2, pp. 90–106, 2023.
[38] A. Mutahhar, T. J. S. Khanzada, and M. F. Shahid, "Enhanced Scalability and Security in Blockchain-Based Transportation Systems for Mass Gatherings," *Information*, vol. 16, no. 8, p. 641, 2025.
[39] A. Zimba, K. O. Phiri, M. Mulenga, and G. Mukupa, "Blockchain Technology and Energy Efficiency: A Systematic Literature Review of Consensus Mechanisms, Architectural Innovations, and Sustainable Solutions," 2025.
[40] S. Inikhov, "A Comparative Study of Cryptocurrency and Traditional Payment Systems in International Trade: A New Trade Theory Perspective," *Bachelor Thesis). Czech Univ. Life Sci. Prague*, 2024.
[41] M. Soud, G. Liebel, and M. Hamdaqa, "A fly in the ointment: an empirical study on the characteristics of Ethereum smart contract code weaknesses," *Empir. Softw. Eng.*, vol. 29, no. 1, p. 13, 2024.
[42] A. Bharadwaj, "Blockchain and the Right to Be Forgotten," *Nirma ULJ*, vol. 11, p. 35, 2021.
[43] D. Mishra and S. Phansalkar, "Blockchain Security in Focus: A Comprehensive Investigation into Threats, Smart Contract Security, Cross-Chain Bridges, Vulnerabilities Detection Tools & Techniques," *IEEE Access*, 2025.