IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

Blockchain Technology: Applications Beyond Cryptocurrency

Pawar S. B., Pokharkar Narendra D., Phapale S. R.
Vidya Niketan Institute of Management & Computer Application, Bota

Abstract: *Blockchain is a distributed digital ledger that records transactions across a network of computers. Although it first became widely known through cryptocurrencies, its properties—such as shared recordkeeping, tamper-evident history, cryptographic verification, and programmable smart contracts—have encouraged research in many non-financial fields. This review paper discusses the potential use of blockchain in supply chain management, healthcare, digital identity, electronic voting, education, and intellectual property management. It also examines important limitations, including scalability, transaction costs, privacy, interoperability, governance, and the difficulty of correcting inaccurate information once it has been recorded. Existing reviews show that blockchain may improve traceability, auditability, and coordination among organizations, but many proposals remain at the prototype or pilot stage. Blockchain is therefore not a universal replacement for traditional databases; it is most useful when several parties need to maintain and verify shared records without fully relying on one central administrator. The paper concludes with future research directions for practical, secure, energy-efficient, and responsible blockchain adoption.*

Keywords: Blockchain, Distributed Ledger, Smart Contracts, Supply Chain, Healthcare, Digital Identity, Data Security

I. INTRODUCTION

A blockchain is a type of distributed ledger in which records are grouped into blocks and linked using cryptographic techniques. Copies of the ledger may be maintained by multiple participants, while a consensus mechanism helps the network agree on valid updates. This structure can make past records difficult to alter without detection. Smart contracts—programs executed according to predefined rules on a blockchain platform—can automate selected processes.

Cryptocurrency was the first widely recognized application of blockchain, but researchers have since explored its use in areas where trust, traceability, and reliable record sharing are important. A systematic literature review by Casino, Dasaklis, and Patsakis classified blockchain applications across areas such as supply chains, healthcare, the Internet of Things, privacy, and data management [1]. Maesa and Mori also reviewed applications including electronic voting, healthcare records, identity management, access control, and supply chains [2].

The purpose of this paper is to review major non-cryptocurrency applications, summarize their possible benefits, identify limitations, and discuss directions for future development. The paper takes a balanced view: blockchain can provide useful shared infrastructure, but its value depends on the specific problem, system design, and quality of the information entered into it.

II. REVIEW APPROACH

This paper uses a narrative review approach based on selected peer-reviewed review articles and research papers about blockchain applications beyond cryptocurrency. The literature considered includes broad systematic reviews and domain-focused studies on healthcare and supply-chain management. The discussion groups the findings by application area and recurring technical or organizational challenges. This is a focused narrative review, not a new systematic review with an exhaustive database search or formal quality scoring.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

III. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

3.1 Distributed and Shared Records

A distributed ledger allows approved participants to consult a shared history of transactions. This can reduce disagreement between separate records, especially when organizations need to exchange information. Depending on the design, a blockchain may be public, allowing broad participation, or permissioned, restricting participation to approved entities.

3.2 Cryptographic Integrity and Traceability

Cryptographic hashes and digital signatures help verify that records have not been changed without authorization. A ledger can provide a traceable history of events, which may support audits and accountability. However, these features do not prove that the original data was true; inaccurate information entered into the system can remain in the record.

3.3 Smart Contracts

Smart contracts execute programmed rules, such as recording an approval after specified conditions are met. They can support workflow automation, but bugs, ambiguous rules, and incorrect external inputs can cause errors. Careful testing, access control, and procedures for resolving disputes are therefore necessary.

IV. APPLICATIONS BEYOND CRYPTOCURRENCY

4.1 Supply Chain Management

Supply chains involve manufacturers, distributors, transport providers, retailers, and customers. Blockchain can record product movement, handovers, certifications, and selected quality checks in a shared history. This may improve traceability, help identify where delays or recalls occurred, and make it harder for one participant to silently rewrite previously recorded events. In practice, benefits depend on reliable data collection, integration with existing systems, and participation by the organizations in the chain. A review of blockchain in healthcare supply chains found substantial research interest but also noted that much of the literature was theoretical or simulation-based, with limited real-world case evidence [3].

4.2 Healthcare and Medical Records

Healthcare organizations need to share information while protecting patient privacy. Blockchain may be used to record consent, access events, document integrity checks, and permissions for exchanging medical information. Sensitive clinical records are generally better stored in controlled databases or secure repositories, with the blockchain holding references, proofs, or audit records rather than unrestricted medical data. A 2024 review discussed potential uses in health-data exchange, consent management, drug supply chains, and clinical trials, while identifying performance and scalability concerns [4]. Recent reviews also emphasize that many designs still need stronger real-world evaluation and clearer governance arrangements [5].

4.3 Digital Identity and Access Management

Blockchain-based identity systems may help users prove selected claims, such as a qualification or membership, without repeatedly depending on a single identity provider. Decentralized identifiers and verifiable credentials can be used with supporting infrastructure to improve control over how identity information is shared. These systems still require safe key recovery, identity verification, privacy safeguards, and standards that allow different providers to work together.

4.4 Electronic Voting

Blockchain has been proposed for recording voting events and supporting auditability in electronic voting systems. A well-designed system would need to protect voter privacy, prevent coercion and duplicate voting, provide accessible participation, and allow independent verification. A blockchain alone cannot guarantee a fair election or protect a compromised voting device. Therefore, any proposed voting system requires careful security analysis, independent audits, and evidence that it meets election requirements.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

4.5 Education and Academic Credentials

Educational institutions may use verifiable digital credentials to issue and validate degrees, certificates, and training records. Employers or other institutions could verify whether a credential was issued by a recognized organization without relying entirely on manual document checks. The issuer's identity, correction and revocation procedures, and protection of student data remain important.

4.6 Intellectual Property and Digital Records

Blockchain can create timestamped evidence that a file, design, or document existed in a particular form at a given time. This may support recordkeeping for creative works, contracts, and licensing workflows. However, a timestamp does not by itself prove authorship, ownership, or legal entitlement. Evidence from the ledger must be considered alongside applicable law and other records.

V. POTENTIAL BENEFITS

Transparency and shared visibility: authorized participants can consult a consistent transaction history.
Tamper-evident records: cryptographic links and signatures can help reveal unauthorized changes.
Traceability: events can be followed across organizations, supporting audits and product recalls.
Workflow automation: smart contracts can execute predefined steps and reduce some manual reconciliation.
Reduced dependence on a single record keeper: selected multi-party processes can operate with shared governance.
Verifiability: digital proofs and credentials can make it easier to check selected records.

VI. CHALLENGES AND LIMITATIONS

6.1 Scalability and Performance

Some blockchain networks process transactions more slowly or at higher cost than centralized databases. Consensus and replication can add latency and storage overhead. The appropriate design depends on the required transaction volume, response time, and trust model.

6.2 Privacy and Data Protection

A permanent or widely replicated record can conflict with confidentiality and data-minimization requirements. Personal or sensitive information should not be placed on a public ledger without careful legal and technical analysis. Permissioned access, encryption, off-chain storage, and privacy-preserving methods may reduce risks but do not remove them automatically.

6.3 Interoperability

Different blockchain platforms may use incompatible data formats, identity models, and smart-contract environments. Connecting them to older databases and business systems can be costly. Common standards and well-defined interfaces are needed for practical adoption.

6.4 Governance, Regulation, and Responsibility

Organizations must decide who can join the network, approve software changes, resolve disputes, and respond to security incidents. Legal responsibilities can be unclear when records are distributed across organizations or countries. Governance should be designed before deployment.

6.5 Data Quality and Human Factors

Blockchain can preserve a record without ensuring that the recorded information is accurate. Sensors can fail, users can make mistakes, and dishonest participants can submit false data. User-friendly interfaces, validation, auditing, and clear accountability are essential.

VII. COMPARISON WITH TRADITIONAL DATABASES

Aspect	Blockchain	Traditional Database
Control	May be shared across several participants	Usually managed by a central owner
Record changes	Past records are designed to be tamper-evident	Authorized administrators can update or delete

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

		records
Performance	May involve consensus and replication overhead	Often faster for routine centralized workloads
Best fit	Multi-party records where shared verification matters	Applications with a trusted operator and frequent updates
Governance	Requires agreement among network participants	Usually determined by the database owner

This comparison is general rather than absolute. Permissioned blockchains and modern databases vary considerably. A blockchain should be selected only when shared verification or multi-party governance provides a clear benefit over a simpler database.

VIII. FUTURE SCOPE

Energy-efficient consensus mechanisms that reduce unnecessary resource consumption.
Improved interoperability between blockchain platforms and established information systems.
Privacy-preserving techniques that enable verification while limiting disclosure of personal data.
More robust smart-contract testing, formal verification, monitoring, and upgrade procedures.
Better governance models for public services, healthcare, education, and multi-organization supply chains.
Long-term field studies that measure cost, usability, security, and operational value rather than relying only on prototypes.

IX. CONCLUSION

Blockchain technology has potential applications well beyond cryptocurrency. Its shared and tamper-evident ledger can support traceability in supply chains, audit trails in healthcare, digital credentials, selected voting designs, and records related to intellectual property. Smart contracts may automate defined processes, while cryptographic verification can make certain records easier to check. Nevertheless, blockchain does not automatically guarantee truth, privacy, legal compliance, or better performance. Scalability, interoperability, governance, data quality, and implementation costs remain important barriers. The most suitable applications are those in which multiple parties need to verify shared records and where the benefits justify the added complexity. Future work should prioritize practical evaluations, responsible data handling, common standards, and clear governance.

REFERENCES

1. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006
2. Di Francesco Maesa, D., & Mori, P. (2020). Blockchain 3.0 applications survey. Journal of Parallel and Distributed Computing, 138, 99–114. https://doi.org/10.1016/j.jpdc.2019.12.019
3. Fiore, M., Capodici, A., Rucci, P., Bianconi, A., Longo, G., Ricci, M., Sanmarchi, F., & Golinelli, D. (2023). Blockchain for the healthcare supply chain: A systematic literature review. Applied Sciences, 13(2), 686. https://doi.org/10.3390/app13020686
4. Kasyapa, M. S. B., & Vanmathi, C. (2024). Blockchain integration in healthcare: A comprehensive investigation of use cases, performance issues, and mitigation strategies. Frontiers in Digital Health, 6, 1359858. https://doi.org/10.3389/fdgth.2024.1359858
5. Chandak, A., Chandak, P., & Soni, N. (2026). Blockchain applications in electronic health records: A systematic review of qualitative and quantitative evidence. BMC Medical Informatics and Decision Making, 26, 176. https://doi.org/10.1186/s12911-026-03476-3