



Blockchain Technology Beyond Cryptocurrency: A Systematic Review of Applications, Challenges, and Emerging Trends

Caroline Peters
Independent Researcher, Australia
Corresponding Author: Caroline Peters, **E-mail:** carolpeters@gmail.com

ARTICLE INFORMATION	ABSTRACT
<p>Submitted: July 02, 2026 Accepted: August 15, 2026 Published: September 30, 2026 Volume: 2 Issue: 1</p> <hr/> <p>KEYWORDS</p> <p>Blockchain technology; decentralized systems; smart contracts; digital transformation; supply chain; cybersecurity</p>	<p>Blockchain technology has evolved beyond its original application in cryptocurrency to become an important digital infrastructure for secure, decentralized, and transparent information management across diverse sectors. This systematic review examines the applications, challenges, and emerging trends associated with blockchain technology beyond cryptocurrency. The review synthesizes recent scholarly literature addressing blockchain adoption and implementation in healthcare, supply chain management, finance, education, government, identity management, energy, the Internet of Things, and other emerging digital environments. The findings indicate that blockchain can enhance data integrity, traceability, transparency, decentralized trust, transaction efficiency, and secure information sharing by enabling tamper-resistant and verifiable records without relying exclusively on centralized intermediaries. Applications are increasingly associated with electronic health records, pharmaceutical traceability, digital credentials, smart contracts, decentralized identity, public-sector services, logistics monitoring, and peer-to-peer energy systems. However, the literature also identifies persistent barriers, including scalability limitations, high computational and infrastructure requirements, interoperability problems, regulatory uncertainty, privacy concerns, cybersecurity vulnerabilities, governance challenges, and limited technical expertise. Emerging trends include the integration of blockchain with artificial intelligence, Internet of Things technologies, decentralized identity systems, tokenization, smart contracts, and energy-efficient consensus mechanisms. Overall, the review demonstrates that blockchain's future value lies less in cryptocurrency speculation and more in its potential to support trusted digital ecosystems and decentralized data infrastructures. Successful adoption will nevertheless depend on technological maturity, appropriate governance frameworks, interoperability standards, regulatory clarity, and context-specific implementation strategies.</p>

1. Introduction

Blockchain technology has evolved from a specialized infrastructure associated primarily with cryptocurrencies into a broader digital technology with potential applications across finance, healthcare, supply-chain management, government, education, energy, intellectual property, and other sectors. Introduced through the Bitcoin architecture, blockchain established a mechanism for maintaining a distributed ledger without relying exclusively on a centralized intermediary. Its core characteristics including decentralization, cryptographic security, transparency, immutability, traceability, and consensus-based validation have subsequently attracted substantial interest from researchers, organizations, governments, and technology developers. As digital transformation increasingly requires secure mechanisms for sharing and verifying information among multiple stakeholders, blockchain has emerged as a potential technological foundation for decentralized trust and data coordination.

The expansion of blockchain beyond cryptocurrency has been driven by the development of programmable and enterprise-oriented blockchain platforms. Smart contracts, for example, enable predefined rules and transactions to be executed automatically when specified conditions are satisfied, creating possibilities for decentralized applications and automated

business processes. Permissioned blockchain networks have also been developed to address situations in which participating organizations require greater control over network membership, transaction visibility, governance, and regulatory compliance (Le, 2021). These developments have broadened the technological scope of blockchain from a digital-payment mechanism toward an infrastructure for managing transactions, identities, records, assets, and interorganizational processes. Consequently, contemporary blockchain research increasingly examines applications in which trust, provenance, coordination, and verifiability are important rather than focusing exclusively on cryptocurrency.

One of the most extensively investigated areas is financial services. Blockchain can facilitate peer-to-peer transactions, cross-border payments, trade finance, digital asset management, and automated settlement while potentially reducing dependence on multiple intermediaries. The emergence of decentralized finance (DeFi) has further demonstrated how blockchain-based smart contracts can support financial services without conventional institutional structures. Beyond finance, blockchain has attracted considerable attention in supply-chain management, where distributed ledgers can provide traceability of products and transactions across complex networks involving manufacturers, distributors, logistics providers, retailers, and consumers. Blockchain-based provenance systems may improve the visibility of product histories and support the verification of information relating to origin, movement, ownership, and compliance. These applications are particularly relevant in sectors where counterfeit products, fragmented information systems, and limited visibility create operational and governance challenges.

Healthcare represents another important domain for blockchain research. Potential applications include secure health-information exchange, electronic health records, medical-data management, patient identity, clinical research, pharmaceutical supply-chain traceability, and consent management. Blockchain's distributed architecture may support controlled data sharing among healthcare stakeholders while providing mechanisms for recording access and maintaining verifiable transaction histories. Nevertheless, healthcare applications also demonstrate an important distinction between blockchain and conventional databases: blockchain does not automatically guarantee data accuracy or confidentiality simply because information is cryptographically recorded. Sensitive health information, scalability requirements, interoperability constraints, and data-protection regulations create significant implementation challenges (Ogayemi, 2026). Similar tensions occur in government and public services, where blockchain has been investigated for digital identity, land and property registries, public records, voting-related systems, taxation, licensing, and administrative processes. The potential benefits of transparency and auditability must, however, be considered alongside privacy, governance, institutional accountability, and legal requirements.

Blockchain applications have also expanded into energy, the Internet of Things (IoT), education, intellectual property, and digital identity. In energy systems, blockchain can support decentralized energy trading and coordination among distributed producers and consumers. In IoT environments, it may provide mechanisms for recording device interactions and establishing trust among heterogeneous devices. Educational applications include credential verification, academic-record management, and decentralized certification, while intellectual-property applications seek to establish verifiable records of ownership and transactions involving digital assets. Digital identity systems similarly explore blockchain-based approaches to user-controlled credentials and verifiable claims. These emerging applications illustrate that the relevance of blockchain increasingly lies not simply in storing cryptocurrency transactions but in its potential to create shared, tamper-evident records among participants who may not fully trust one another.

Despite these opportunities, the literature increasingly emphasizes that blockchain adoption is accompanied by substantial technical, organizational, economic, legal, and ethical challenges. Scalability remains a major concern because some blockchain architectures face limitations in transaction throughput, latency, and storage requirements as network activity increases. Energy consumption has also been an important concern for blockchain systems that rely on energy-intensive consensus mechanisms, although alternative mechanisms such as proof-of-stake have changed the sustainability profile of some newer networks. Interoperability represents another persistent challenge because blockchain platforms may employ different protocols, data structures, governance arrangements, and standards. The integration of blockchain with existing enterprise systems can therefore require significant technical and organizational investment.

Security and privacy present additional complexities. Although cryptographic mechanisms can strengthen the integrity of recorded transactions, blockchain systems are not immune to vulnerabilities involving smart contracts, private-key management, network governance, implementation errors, or connected applications. The apparent immutability of blockchain records can also create tensions with privacy and data-governance principles when sensitive or personally identifiable information is permanently recorded. Furthermore, the decentralization of technological infrastructure does not necessarily eliminate centralized forms of control (Miraz, 2018). Developers, validators, exchanges, platform operators, consortium members, and governance communities can exercise significant influence over blockchain ecosystems. Therefore, claims concerning decentralization and trust require careful consideration of the particular architecture, governance model, and institutional environment in which a blockchain system operates.

Regulatory and legal uncertainty further complicates blockchain implementation. Blockchain networks frequently operate across national jurisdictions, while laws governing financial services, data protection, consumer rights, taxation, digital assets, electronic transactions, and intellectual property are generally administered within particular legal systems. Smart contracts may automate transactions, but their legal status and enforceability can vary according to jurisdiction and contractual context. Organizations considering blockchain adoption must consequently evaluate not only technological feasibility but also compliance, governance, accountability, and risk. These issues suggest that blockchain should not be regarded as a universally applicable replacement for conventional information systems. Rather, its value depends on whether its specific characteristics address a genuine coordination, trust, provenance, or verification problem better than available alternatives.

The rapid diversification of blockchain applications has generated a large and increasingly fragmented body of research. Existing studies have examined particular sectors, technological architectures, consensus mechanisms, smart contracts, security issues, and implementation challenges. However, the expansion of blockchain into multiple domains makes it increasingly important to synthesize evidence across application areas while simultaneously examining technological limitations and emerging developments. A systematic review can help identify recurring application patterns, distinguish established uses from emerging experimental applications, and clarify the relationships between blockchain capabilities and sector-specific requirements. It can also reveal areas where evidence remains predominantly conceptual or exploratory rather than supported by large-scale empirical implementation.

Against this background, this systematic review examines blockchain technology beyond cryptocurrency, focusing on its applications, challenges, and emerging trends across contemporary technological and organizational contexts. The review synthesizes the literature on major non-cryptocurrency applications, examines the technological and institutional factors influencing blockchain adoption, identifies recurring limitations and risks, and evaluates emerging directions shaping the field (Sunny, 2022). Particular attention is given to smart contracts, decentralized applications, permissioned blockchain, tokenization, decentralized identity, blockchain-IoT integration, interoperability, sustainability, privacy, and blockchain-enabled digital ecosystems. By bringing these strands of research together, the study seeks to provide a comprehensive understanding of how blockchain is evolving from a cryptocurrency-supporting technology into a broader infrastructure for decentralized data management, digital trust, and interorganizational coordination.

2. Methodology

2.1 Research Design

This study adopted a systematic literature review design to critically examine the development, applications, challenges, and emerging trends associated with blockchain technology beyond its original cryptocurrency-oriented application. A systematic review was considered appropriate because blockchain research has expanded across diverse domains, including healthcare, supply-chain management, finance, education, governance, energy, Internet of Things (IoT), intellectual property, and digital identity. The review synthesized existing scholarly evidence to identify dominant application areas, technological benefits, persistent limitations, and emerging directions in blockchain research. The methodological approach emphasized transparency, reproducibility, and consistency in the identification, screening, selection, and synthesis of relevant studies.

2.2 Review Objectives and Research Questions

The review was guided by the overall objective of establishing how blockchain technology is being applied beyond cryptocurrency and what technological, organizational, regulatory, and social factors influence its adoption. Specifically, the review examined the principal non-cryptocurrency applications of blockchain, the benefits associated with blockchain-enabled systems, the major technical and institutional challenges limiting implementation, and emerging trends that are shaping the future development of blockchain-based solutions. The review was guided by the following research questions: What are the major applications of blockchain technology beyond cryptocurrency? What benefits are reported from blockchain adoption across different sectors? What technological, organizational, regulatory, and security challenges affect blockchain implementation? What emerging trends are shaping the future development and application of blockchain technology?

2.3 Literature Search Strategy

A comprehensive literature search was conducted using major academic databases and scholarly search platforms relevant to computer science, information systems, engineering, business, and interdisciplinary technology research. The search strategy focused on publications addressing blockchain applications outside conventional cryptocurrency and digital-currency contexts. Search terms were developed from the main concepts of the study and combined using Boolean operators. Representative search expressions included "blockchain technology" AND "applications," "blockchain" AND "healthcare," "blockchain" AND "supply chain," "blockchain" AND "Internet of Things," "blockchain" AND "smart contracts," "blockchain" AND "digital identity," "blockchain" AND "governance," and "blockchain" AND "challenges" OR "emerging trends." Additional combinations involving

decentralization, distributed ledger technology, interoperability, scalability, privacy, security, sustainability, and enterprise blockchain were used to capture studies employing different terminology.

2.4 Eligibility Criteria

Studies were considered eligible when they directly examined blockchain or distributed-ledger technologies and provided substantive discussion of applications, benefits, challenges, adoption, implementation, or emerging developments beyond cryptocurrency. Peer-reviewed journal articles, conference papers, systematic reviews, conceptual studies, and relevant empirical research were considered where they contributed meaningful evidence to the research questions. Publications were excluded when their primary focus was cryptocurrency price prediction, speculative trading, cryptocurrency investment behavior, or purely financial-market analysis without meaningful consideration of broader blockchain applications. Duplicate records, publications lacking sufficient scholarly information, non-academic commentary, and studies unrelated to the objectives of the review were also excluded.

2.5 Study Selection and Screening

The retrieved literature was subjected to a structured screening process involving identification, duplicate removal, title and abstract screening, full-text assessment, and final inclusion. During the initial screening stage, records were examined to determine their relevance to blockchain applications, challenges, or emerging technological developments. Studies that clearly focused exclusively on cryptocurrency-related issues were removed. The abstracts and keywords of potentially relevant studies were subsequently assessed against the predefined eligibility criteria. Full-text articles were then examined to establish whether they contained sufficient information relevant to at least one of the research questions. Only studies meeting the inclusion criteria and demonstrating substantive relevance to the review were retained for synthesis. The screening procedure was conceptually aligned with established systematic-review reporting practices, particularly the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework.

2.6 Quality Assessment of Selected Studies

The methodological and conceptual quality of the selected literature was assessed before synthesis. Particular attention was given to the clarity of research objectives, appropriateness of research design, transparency of methods, adequacy of evidence, clarity of findings, and relevance to blockchain applications beyond cryptocurrency. For empirical studies, consideration was also given to the suitability of sampling procedures, data-collection methods, analytical approaches, and reporting of limitations. Review and conceptual papers were assessed in terms of the clarity of their analytical framework, breadth of literature coverage, logical consistency, and contribution to understanding blockchain development. Studies providing insufficient methodological information or weak relevance to the research questions were given lower priority during synthesis.

2.7 Data Extraction

Relevant information was systematically extracted from the selected publications and organized according to the objectives of the review. The extraction process captured bibliographic information, publication characteristics, research context, blockchain technology or architecture examined, application sector, principal use case, reported benefits, implementation requirements, challenges, and emerging technological developments. Particular attention was given to recurring concepts such as decentralization, transparency, traceability, immutability, smart contracts, data integrity, privacy, scalability, interoperability, energy consumption, governance, and regulatory compliance. Extracted evidence was subsequently compared across studies to identify similarities, differences, patterns, and research gaps.

2.8 Data Synthesis and Analysis

A qualitative thematic synthesis approach was employed to integrate findings from the selected studies. The analysis involved grouping the literature according to major application domains and then identifying recurring technological benefits, implementation barriers, and emerging trends within and across those domains. Application areas were synthesized into broad categories such as healthcare, supply-chain and logistics, financial services beyond cryptocurrency, public administration and governance, education, energy, IoT, digital identity, intellectual property, and other emerging domains. Challenges were analyzed thematically across technical, security, privacy, organizational, economic, legal, regulatory, and environmental dimensions. Emerging trends were examined in relation to developments such as blockchain interoperability, blockchain–AI integration, decentralized identity, tokenization of real-world assets, enterprise blockchain, Web3 architectures, privacy-enhancing technologies, and more sustainable consensus mechanisms.

2.9 Reporting and Transparency

The review findings were organized to provide a coherent account of the evolution and diversification of blockchain technology beyond cryptocurrency. The selection and synthesis processes were documented systematically to enhance methodological transparency and reduce the possibility of arbitrary inclusion of literature. Where appropriate, the review distinguished between

established applications supported by substantial research evidence and emerging applications that remain at experimental, pilot, or early-adoption stages. This distinction was important because blockchain research spans mature implementations as well as rapidly evolving technological concepts whose long-term effectiveness and scalability remain uncertain.

2.10 Ethical Considerations

As this study relied exclusively on previously published literature and did not involve human participants, personal data, interviews, experiments, or direct interaction with research subjects, formal primary-data ethical approval was not required. Nevertheless, the review adhered to principles of academic integrity through appropriate attribution of previous research, accurate representation of reported findings, avoidance of plagiarism, and transparent reporting of the review methodology. The interpretation of evidence was undertaken with attention to differences in research contexts, methodological approaches, technological maturity, and limitations reported by the original studies.

3. Findings and Discussion

The systematic review identified blockchain technology as a multi-sectoral infrastructure with applications extending substantially beyond cryptocurrency and speculative digital assets. Across the reviewed literature, the principal value propositions were transparency, immutability, traceability, decentralized verification, automated execution through smart contracts, and the creation of shared records among organizations that may not fully trust one another. However, the evidence also indicates that blockchain does not automatically improve institutional or operational outcomes. Its effectiveness depends on the quality of data entered into the system, governance arrangements, interoperability with existing information systems, scalability, privacy protection, regulatory acceptance, and the incentives of participating organizations. The findings therefore position blockchain less as a universal replacement for conventional databases and more as a distributed coordination and verification mechanism that can be valuable where multiple actors require a common, auditable record.

3.1 Blockchain Applications Beyond Cryptocurrency

3.1.1 Blockchain in Supply Chain Management and Logistics

A major application identified in the literature concerns supply-chain management, where blockchain is used to establish a shared and tamper-resistant record of transactions and product movements. Conventional supply chains frequently involve fragmented information systems operated by suppliers, manufacturers, logistics providers, wholesalers, retailers, regulators, and consumers. This fragmentation can make it difficult to determine the origin, ownership, location, and handling history of products. Blockchain can address part of this problem by recording time-stamped transactions that can be accessed and verified by authorized participants. The resulting visibility can support product provenance, inventory coordination, transaction verification, and faster identification of problematic batches (Gad, 2022). The literature particularly emphasizes food and pharmaceutical supply chains because traceability is closely connected to public safety. For example, a blockchain-based food system can record information about production, processing, transportation, storage, and retail distribution, enabling participants to trace a product through successive stages of the value chain.

The reviewed evidence suggests that the strongest contribution of blockchain in logistics is not simply the storage of information but the creation of a common information environment across organizational boundaries. Smart contracts can further automate processes such as confirmation of delivery, compliance checks, payment release, and documentation. In international trade, this can reduce dependence on paper-based documentation and improve visibility among exporters, importers, banks, customs authorities, insurers, and logistics providers. Similar applications have been explored in pharmaceutical supply chains to strengthen the verification of medicines and reduce opportunities for counterfeit products to enter legitimate distribution channels. In agriculture, blockchain can connect farmers, processors, distributors, and consumers through verifiable records concerning origin, certification, production practices, and transportation. Nevertheless, the literature repeatedly identifies the “garbage-in, garbage-out” problem: an immutable blockchain record cannot guarantee that information entered at the beginning of a supply chain is truthful. Consequently, blockchain should be combined with trusted data-entry procedures, Internet-of-Things sensors, certification systems, and regulatory oversight rather than treated as a standalone solution.

3.1.2 Blockchain in Healthcare and Medical Data Management

Healthcare emerged as another important application area, particularly in relation to electronic health records, medical-data exchange, patient identity, pharmaceutical traceability, and clinical research. Healthcare information is typically distributed across hospitals, laboratories, pharmacies, insurance organizations, specialist practices, and public-health agencies, creating interoperability and data-sharing challenges. Blockchain can provide a shared audit trail through which authorized participants can verify when information was created, modified, accessed, or transferred (Nandanwar, 2023). This capability has implications for maintaining data integrity and accountability, particularly where multiple institutions need to exchange information without relying entirely on a single centralized administrator.

The findings indicate that blockchain may also strengthen patient-centered control over health information by allowing patients to participate in decisions concerning access to their records. Blockchain-enabled identity mechanisms can potentially link authorized users to verified medical information while maintaining an auditable history of data access. In pharmaceutical management, the technology can support medicine provenance and verification from manufacturers through distributors to healthcare providers. In clinical research, blockchain has been proposed for documenting research-data provenance, consent processes, study protocols, and the integrity of research records. These applications correspond with earlier research emphasizing blockchain's potential to address trust and interoperability problems in health-information ecosystems. At the same time, the evidence demonstrates that healthcare is a particularly difficult environment for blockchain deployment because medical information is highly sensitive. Storing personal health information directly on an immutable ledger may conflict with privacy requirements and data-correction or deletion requirements. Consequently, many proposed architectures favor storing sensitive information off-chain while using blockchain to record permissions, hashes, transactions, or references (Gad, 2022). Scalability, interoperability with existing electronic health-record systems, computational costs, and governance among healthcare institutions remain important barriers to large-scale implementation.

3.1.3 Blockchain in Finance, Banking, and Digital Payments

Beyond cryptocurrency, financial services represent one of the most mature fields of blockchain experimentation. The review identified applications in cross-border payments, trade finance, clearing and settlement, digital assets, smart contracts, fraud management, and decentralized financial services. Traditional cross-border transactions may involve several intermediaries, including correspondent banks, payment networks, clearing institutions, and regulatory authorities. Blockchain-based systems can potentially reduce the number of reconciliation steps by enabling participants to share a synchronized transaction record. This may improve transaction visibility and shorten settlement processes, particularly where institutions currently maintain separate ledgers that must be reconciled.

Blockchain-based smart contracts also have implications for trade finance because contractual conditions can be connected to documentary or transactional events. For instance, payment could be automatically initiated after predefined conditions concerning shipment, delivery, or document verification have been satisfied. Similarly, blockchain can facilitate tokenized representations of financial or real-world assets and support more programmable forms of settlement (Romano, 2021). The literature reports potential improvements in transparency and operational efficiency, but the magnitude of cost reductions varies considerably across use cases. Blockchain does not necessarily eliminate intermediaries or transaction costs because compliance, identity verification, governance, cybersecurity, and regulatory requirements remain necessary. Moreover, decentralized finance introduces additional risks involving smart-contract vulnerabilities, market instability, consumer protection, and regulatory uncertainty. The evidence therefore supports blockchain as a mechanism for redesigning financial processes rather than as an automatic replacement for established banking infrastructure.

3.2 Blockchain Applications in Public and Institutional Services

3.2.1 Blockchain in Government and Public Administration

The review identified government and public administration as significant areas in which blockchain is being explored to improve record integrity, transparency, and administrative coordination. Potential applications include public registries, procurement, taxation, welfare distribution, licensing, government transactions, and administrative records. Government agencies frequently operate large databases containing information about citizens, businesses, property, taxes, benefits, and public expenditure. Where several agencies need access to common information, distributed ledgers can provide a shared record and an auditable history of transactions. This can reduce inconsistencies between institutional databases and make unauthorized alteration of records more difficult.

Public procurement illustrates the potential particularly clearly. Blockchain-based procurement systems can record tender submissions, contractual milestones, payments, and supplier interactions in an auditable sequence. Similarly, welfare systems can potentially use smart contracts to automate the distribution of benefits once predefined eligibility conditions have been verified. Tax administration could use distributed records to improve transaction visibility and reduce reconciliation problems between taxpayers, businesses, financial institutions, and government agencies (Khan, 2021). However, the reviewed literature does not support the assumption that blockchain automatically eliminates corruption or administrative inefficiency. Governance remains critical because authorities determine which participants can write to the system, which information is publicly visible, how disputes are resolved, and how erroneous records are corrected. Blockchain can make records more difficult to alter retrospectively, but it cannot independently determine whether an original transaction was legitimate.

3.2.2 Blockchain in Digital Identity, Voting, and Public Records

Digital identity and public-record management constitute another prominent application domain. Blockchain-based identity systems can provide verifiable credentials that individuals can present to different organizations without requiring each

institution to maintain an independent copy of the underlying record. This approach may be particularly useful for professional licenses, educational qualifications, government credentials, and other forms of digitally verifiable identity. Similarly, blockchain has been explored for land registries because property ownership depends on reliable historical records of transactions, transfers, and claims. A distributed ledger could provide a transparent chronology of ownership changes and reduce disputes associated with inconsistent or fragmented records.

Electronic voting has also attracted substantial blockchain research because immutable transaction records appear compatible with requirements for auditability and verifiability. Blockchain-based voting proposals seek to create independently verifiable records while limiting opportunities for unauthorized alteration. Nevertheless, the review indicates that voting is considerably more complex than simply recording votes on an immutable ledger. Election systems must protect voter privacy, ensure eligibility, prevent coercion and vote buying, guarantee accessibility, accommodate lost or compromised credentials, and maintain secure procedures from voter registration through vote counting (Yli-Huumo, 2016). Blockchain does not itself solve these problems. Consequently, while the technology can contribute to auditability in carefully designed systems, questions concerning endpoint security, identity management, privacy, governance, and public trust remain central.

3.2.3 Blockchain in Education, Research, and Credential Verification

In education and research, blockchain applications are concentrated around credential verification, student records, micro-credentials, intellectual-property management, and research-data provenance. Traditional academic credentials often require verification by universities, employers, professional bodies, or other institutions. Blockchain-based credentials can create digitally verifiable records that allow authorized parties to confirm the authenticity and issuing institution of a qualification. This can be particularly useful for graduates who move between countries or employment systems, where conventional verification may be slow and administratively burdensome. Micro-credentials and short-course certificates can similarly be recorded as portable digital achievements.

The literature also identifies potential applications in research administration. Blockchain can create provenance records for datasets, document successive contributions to research outputs, timestamp intellectual-property claims, and provide auditable records of data sharing. These functions may strengthen confidence in the history and integrity of scholarly materials. However, blockchain-based educational records still depend on recognition by institutions and employers; a technically verifiable credential does not automatically establish substantive equivalence or professional validity (Abrar, 2024). Privacy is also important because educational records contain personal information that should not necessarily be permanently exposed on a distributed ledger. Thus, the evidence supports blockchain primarily as a verification and provenance infrastructure rather than as a replacement for educational institutions' accreditation and quality-assurance functions.

3.3 Blockchain Applications in Emerging Digital and Economic Sectors

3.3.1 Blockchain in Energy and Decentralized Energy Systems

Energy is an increasingly important emerging application of blockchain, particularly as electricity systems become more decentralized through solar panels, batteries, electric vehicles, and other distributed energy resources. The reviewed literature identifies peer-to-peer electricity trading as a principal application. In such systems, blockchain can record transactions between energy producers and consumers and use smart contracts to automate settlement according to predefined rules. A household with excess solar generation, for example, could potentially sell surplus electricity to another participant within a local energy network, with the transaction recorded on a shared ledger.

Blockchain can also support renewable-energy certificates and energy provenance by providing records linking energy attributes to specific production or trading events. This may improve transparency in renewable-energy markets and sustainability claims. Smart contracts can automate payments and other contractual processes, while distributed ledgers can facilitate coordination among producers, consumers, aggregators, and grid operators (Aggarwal, 2023). Nevertheless, the review shows that blockchain-based energy systems face challenges involving transaction throughput, regulatory requirements, integration with physical electricity infrastructure, privacy, energy consumption associated with some consensus mechanisms, and the need for reliable real-time data. Consequently, blockchain's contribution is most evident at the coordination and transaction layer rather than at the physical generation or transmission layer itself.

3.3.2 Blockchain in Real Estate, Intellectual Property, and Digital Assets

The review found growing interest in blockchain for real estate, intellectual property, and digital assets because these domains depend heavily on reliable ownership and transaction records. In real estate, blockchain can potentially support land registration, property histories, ownership transfers, and automated contractual arrangements. Smart contracts could link payment to predefined transfer conditions, reducing manual reconciliation and potentially shortening transaction processes. Tokenization

can also create digital representations of interests in assets, although the legal relationship between a token and an underlying physical property depends on the relevant jurisdiction and contractual framework.

Intellectual-property applications similarly focus on establishing time-stamped evidence of creation, licensing, ownership, and subsequent transfers. Artists, researchers, designers, and other creators can potentially use blockchain records to establish provenance and automate royalty arrangements. Digital assets extend this concept by allowing ownership or usage rights to be represented through blockchain-based tokens. The findings nevertheless indicate that technical ownership of a token should not be confused with legal ownership of an underlying asset. Legal enforceability, copyright law, licensing arrangements, consumer protection, and dispute-resolution mechanisms remain external to the blockchain protocol. Therefore, blockchain can strengthen the evidentiary and transactional infrastructure surrounding property and intellectual property, but its effectiveness depends on integration with established legal institutions.

3.3.3 Blockchain in Agriculture, Food Systems, and Environmental Sustainability

Agriculture, food systems, and environmental sustainability represent an important convergence between blockchain and broader efforts to establish trustworthy provenance and sustainability information. In agricultural value chains, blockchain can record information about production locations, farming practices, certifications, processing, transportation, and final distribution (Wenhua, 2023). Such records may help consumers, regulators, retailers, and certification organizations verify claims concerning origin, organic production, fair trade, or other sustainability attributes. For farmers and producer organizations, transparent records may also improve coordination with buyers and financial institutions.

Environmental applications include carbon markets, renewable-energy certification, sustainability reporting, and environmental monitoring. Blockchain can provide a shared record of carbon-credit issuance, transfer, and retirement, potentially reducing duplicate claims and improving transaction traceability. In sustainability reporting, distributed records can connect environmental claims to underlying data and create an auditable history of reported activities. However, the review identifies a critical limitation: blockchain can preserve and distribute environmental information, but it cannot independently verify whether that information accurately represents physical environmental conditions. Reliable sensors, independent audits, satellite observations, certification mechanisms, and trusted measurement systems therefore remain necessary. The overall evidence suggests that blockchain can strengthen trust and accountability in agricultural and environmental value chains when combined with credible data-generation and verification mechanisms.

3.4 Challenges and Limitations of Blockchain Adoption

The systematic review indicates that the expansion of blockchain beyond cryptocurrency is constrained less by the basic concept of distributed ledgers than by the technical, organizational, regulatory, and economic conditions required for deployment at scale. Across the reviewed literature, scalability, interoperability, privacy, security, energy consumption, implementation cost, governance, and regulatory uncertainty repeatedly emerged as interconnected barriers. The evidence also suggests that the severity of these challenges varies according to blockchain architecture, consensus mechanism, application domain, and degree of integration with existing information systems (Le, 2021). Consequently, blockchain adoption should not be understood as a straightforward technological substitution but as a complex process involving infrastructure redesign, institutional coordination, data governance, and organizational transformation.

3.4.1 Scalability, Interoperability, and Technical Limitations

Scalability was one of the most consistently identified technical limitations. Conventional blockchain architectures can experience restrictions in transaction throughput, confirmation latency, and network capacity when transaction volumes increase. These limitations become particularly important in supply-chain management, healthcare, financial services, IoT, and other environments in which thousands or millions of transactions may need to be processed rapidly. Public blockchains that prioritize extensive decentralization and consensus across geographically distributed participants can experience congestion and higher transaction-processing delays during periods of intensive activity. This creates an important tension among decentralization, security, and performance because increasing processing capacity without compromising the distributed character of the network remains technically challenging.

The reviewed literature nevertheless demonstrates that blockchain architectures are evolving to address these limitations. Permissioned or consortium blockchains, in which participation is restricted to verified organizations, can achieve higher throughput and lower latency because consensus does not have to be established across an unrestricted population of anonymous participants. Such architectures are particularly relevant to interorganizational applications such as banking, healthcare information exchange, logistics, and government services. Layer-two mechanisms, sidechains, sharding, rollups, and other off-chain or parallel-processing approaches similarly seek to reduce the computational burden placed on the underlying blockchain. However, these solutions can introduce additional architectural complexity, new trust assumptions, or interoperability

requirements (Ogayemi, 2026). The evidence therefore suggests that there is no universally optimal blockchain architecture; rather, technical design needs to be aligned with the transaction volume, latency requirements, governance structure, and trust relationships of the application.

Storage requirements represent another important limitation. In conventional distributed-ledger designs, transaction records may be replicated across numerous participating nodes, potentially increasing storage requirements as the ledger grows. This can restrict participation for organizations or devices with limited computational and storage resources. The problem is particularly relevant to IoT environments, where large numbers of resource-constrained devices generate continuous streams of data. Consequently, recent research increasingly explores lightweight blockchain implementations, off-chain storage, edge computing, and hybrid architectures in which only transaction proofs or essential metadata are maintained on-chain while larger datasets remain in external databases or distributed storage systems.

Interoperability constitutes a related but distinct challenge. Blockchain systems often operate according to different protocols, data structures, consensus mechanisms, identity models, and smart-contract environments. As a result, information recorded on one blockchain may not be readily transferable to another without specialized interoperability mechanisms. This is particularly problematic when organizations already operate heterogeneous enterprise systems. A hospital, logistics company, financial institution, or government agency may need blockchain infrastructure to communicate with enterprise resource planning systems, electronic records, cloud platforms, databases, and legacy applications. The reviewed evidence suggests that successful adoption therefore depends not simply on deploying a blockchain but on establishing reliable interfaces between blockchain networks and existing digital infrastructures. Application programming interfaces, interoperability protocols, cross-chain mechanisms, middleware, and standardized data formats can reduce these barriers, but they also create additional points of technical and governance dependence.

3.4.2 Security, Privacy, and Regulatory Challenges

The reviewed literature demonstrates that blockchain provides important security properties, including cryptographic verification, tamper-evident records, distributed validation, and resistance to unauthorized alteration under appropriate network conditions. However, these properties should not be confused with complete system security. A blockchain network may protect the integrity of records while vulnerabilities remain in smart contracts, wallets, application interfaces, identity-management systems, bridges, or other components surrounding the underlying ledger (Miraz, 2018). This distinction is particularly important because many high-profile blockchain incidents have resulted from weaknesses in applications and interfaces rather than from the fundamental cryptographic principles of distributed ledgers.

Smart-contract vulnerabilities represent a significant concern. Because smart contracts can automatically execute predefined rules, programming errors may produce unintended transactions or make assets inaccessible. Bugs in contract logic, inadequate testing, flawed access-control mechanisms, and vulnerabilities in externally connected components can therefore undermine the security of blockchain-based applications. The problem becomes more significant when smart contracts are used in financial services, automated supply-chain processes, healthcare applications, or decentralized organizational structures. Formal verification, independent code auditing, secure development practices, automated testing, and continuous monitoring have consequently become important components of responsible blockchain deployment.

Privacy presents an additional challenge because transparency and immutability can conflict with requirements for confidential information and data deletion. Although blockchain records can be pseudonymous, pseudonymity does not necessarily provide complete anonymity. Transaction patterns and information linked to external datasets may permit identification of participants. The permanent nature of blockchain records can also create difficulties where individuals or organizations have legal rights to modify, correct, or delete personal information. This issue is particularly significant in healthcare, education, financial services, and government applications where blockchain may process personally identifiable or sensitive information. The literature therefore increasingly supports privacy-preserving approaches such as zero-knowledge proofs, selective disclosure, off-chain storage, encryption, permissioned access, and privacy-enhancing cryptographic mechanisms.

Governance is closely connected to both security and privacy. Decentralized systems require mechanisms for determining how software upgrades, disputed transactions, protocol changes, participant admission, and security incidents are handled. In permissioned networks, governance can be more straightforward because participating organizations can establish formal rules and responsibilities; however, this can also reduce decentralization and introduce institutional power asymmetries (Sunny, 2022). Public networks face different challenges because decisions may involve developers, validators, token holders, application providers, and other stakeholders with competing interests. The findings consequently indicate that decentralization does not eliminate governance; instead, it changes where governance authority is located and how it is exercised.

Regulatory uncertainty further complicates adoption. Blockchain applications can simultaneously involve data protection, financial regulation, consumer protection, taxation, cybersecurity, intellectual property, electronic transactions, and cross-border compliance. Regulatory treatment can also differ across jurisdictions, creating uncertainty for organizations operating internationally. This is particularly relevant to tokenized assets, decentralized finance, digital identity, and cross-border data exchange. The reviewed literature therefore identifies regulatory clarity and harmonization as important conditions for institutional adoption. At the same time, regulation must address genuine risks without unnecessarily restricting beneficial technological experimentation. The central challenge is developing governance and compliance frameworks that recognize the technical characteristics of blockchain while maintaining accountability, consumer protection, privacy, and security.

3.4.3 Energy Consumption, Cost, and Organizational Barriers

Energy consumption is a major concern particularly for blockchain networks using proof-of-work consensus. The computational competition required by proof-of-work can generate substantial electricity demand, making this model difficult to reconcile with sustainability objectives when used at large scale. The literature therefore increasingly distinguishes between consensus mechanisms rather than treating blockchain energy consumption as a uniform characteristic of the technology. Proof-of-stake and other alternative mechanisms can substantially reduce the computational requirements associated with transaction validation, while permissioned networks may use more efficient consensus mechanisms because participants are known and governance structures are established (Gad, 2022). Nevertheless, lower energy consumption does not automatically eliminate other environmental or infrastructural costs, including hardware production, data-center requirements, and network infrastructure.

Economic cost also remains an important adoption barrier. Initial implementation can require investment in blockchain infrastructure, cybersecurity, system integration, software development, staff training, auditing, and regulatory compliance. Organizations may also incur continuing costs associated with network governance, upgrades, monitoring, data storage, interoperability, and technical support. These costs can be difficult to justify where blockchain provides only marginal improvements over conventional databases. The evidence consequently suggests that blockchain adoption should be preceded by a clear assessment of the specific problem being addressed, the expected efficiency or trust benefits, and the total cost of ownership.

Organizational barriers are equally significant. Blockchain adoption frequently requires collaboration among multiple organizations rather than decisions by a single firm. Participants must agree on data standards, access rights, governance rules, liability arrangements, technical protocols, and mechanisms for resolving disputes. This can be particularly challenging in supply chains and interorganizational information systems where participants have different commercial interests and technological capabilities. Organizational resistance may also emerge when employees perceive blockchain as threatening established roles, procedures, or decision-making authority. Successful implementation therefore requires change management, leadership support, employee participation, and appropriate technical training.

The shortage of specialized skills further reinforces these barriers. Effective blockchain implementation requires expertise in distributed systems, cryptography, cybersecurity, software engineering, smart-contract development, data governance, and regulatory compliance. Smaller organizations may have difficulty recruiting or retaining personnel with this combination of skills. The findings indicate that capacity building is consequently an important component of adoption strategies. Universities, professional organizations, technology providers, and governments can contribute through specialized training, research partnerships, certification programs, and knowledge-sharing initiatives.

Taken together, the evidence suggests that blockchain adoption is influenced by a combination of technological efficiency, environmental sustainability, economic feasibility, and organizational readiness. The comparison of consensus mechanisms further demonstrates that trade-offs remain unavoidable: energy-efficient mechanisms may introduce different governance or security considerations, while highly decentralized systems may involve greater performance and resource requirements. Blockchain therefore appears most viable when organizations undertake a comprehensive assessment of technical, economic, environmental, and institutional conditions before implementation.

3.5 Emerging Trends and Future Directions in Blockchain Technology

The systematic review identifies a transition from blockchain as primarily a cryptocurrency-supporting infrastructure toward a broader digital infrastructure for trusted data exchange, programmable transactions, digital assets, decentralized applications, and interorganizational coordination. Emerging research increasingly examines blockchain in combination with artificial intelligence, IoT, cloud and edge computing, tokenization, decentralized finance, and Web3 architectures (Nandanwar, 2023). These developments suggest that the future significance of blockchain may depend less on the ledger in isolation and more on its ability to operate as a trusted coordination layer within larger digital ecosystems.

3.5.1 Integration of Blockchain with Artificial Intelligence, IoT, and Other Technologies

The convergence of blockchain and artificial intelligence represents an important emerging research direction. AI systems depend heavily on access to reliable, sufficiently high-quality data, while blockchain can provide mechanisms for recording data provenance, verifying transactions, and establishing audit trails. Their combination may therefore support environments in which data used to train or operate AI systems can be associated with verifiable sources and controlled access rights. For example, in healthcare, blockchain could record the provenance and permission status of clinical datasets while AI systems analyze those datasets for diagnostic or predictive purposes. Similarly, in supply chains, blockchain-based records could provide traceable information about products while AI models identify demand patterns, anomalies, or logistical risks.

The integration of blockchain with IoT presents another important opportunity. IoT environments generate large volumes of machine-produced data and involve devices that may need to communicate without continuous human intervention. Blockchain can provide a shared record of device identities, transactions, permissions, and data exchanges, while smart contracts may automate predefined interactions among devices. In an industrial environment, for example, sensors could transmit verified production information while smart contracts trigger authorized actions when predetermined conditions are met. This creates possibilities for machine-to-machine transactions and automated resource coordination.

However, the review also identifies important limitations in blockchain-IoT integration. Many IoT devices have restricted processing power, storage capacity, and energy availability, making conventional blockchain participation impractical. This has encouraged research into edge computing, lightweight consensus mechanisms, off-chain processing, and hierarchical architectures (Romano, 2021). In these models, computationally constrained devices can interact with edge or gateway nodes that perform more demanding blockchain-related functions. Such architectures may improve scalability and responsiveness but can also create new dependencies and potential points of failure.

Cloud computing and big-data technologies further extend this convergence. Cloud infrastructure can provide scalable computational and storage resources for blockchain applications, whereas blockchain can contribute data provenance and integrity mechanisms for distributed datasets. Edge-cloud-blockchain architectures may therefore support applications requiring both rapid local processing and trusted cross-organizational data exchange. Nevertheless, the literature indicates that technical integration alone does not guarantee trustworthy outcomes. Data entered into a blockchain can remain incorrect even when the ledger subsequently preserves it accurately. This reinforces the importance of data-quality mechanisms, trusted sensors, identity systems, and human oversight.

3.5.2 Decentralized Finance, Tokenization, and Web3 Ecosystems

The reviewed literature indicates that decentralized finance has expanded blockchain applications into programmable financial services, including decentralized exchanges, lending, borrowing, automated market mechanisms, and other forms of financial coordination. These systems demonstrate how smart contracts can automate financial transactions without relying on conventional intermediaries for every operational step. However, the evidence also identifies substantial risks involving smart-contract vulnerabilities, market volatility, governance concentration, oracle dependence, liquidity risks, consumer protection, and regulatory uncertainty. DeFi therefore illustrates both the functional potential of programmable blockchain systems and the difficulty of governing complex decentralized ecosystems.

Tokenization represents another significant development because blockchain can be used to create digital representations of rights or claims associated with assets and other forms of value. Tokenized real-world assets may include financial instruments, property interests, commodities, intellectual property rights, or other assets, depending on the legal and technical structure of the arrangement. Tokenization can potentially improve transferability, fractional ownership, settlement efficiency, transparency, and programmability (Khan, 2021). Its effectiveness, however, depends on the relationship between the blockchain representation and the underlying legal or physical asset. A token does not automatically establish ownership merely because it exists on a blockchain; enforceability depends on contractual arrangements, applicable law, custodial structures, and reliable mechanisms connecting on-chain records with off-chain reality.

The emergence of decentralized applications and decentralized autonomous organizations further demonstrates the movement toward broader Web3 ecosystems. Decentralized applications can combine smart contracts, digital identity, token-based incentives, and distributed data services. DAOs, meanwhile, experiment with collective decision-making through programmable governance mechanisms. These arrangements may facilitate new forms of collaboration and community participation, but the review identifies unresolved questions concerning voting concentration, accountability, legal status, dispute resolution, cybersecurity, and the representation of stakeholder interests. In practice, many supposedly decentralized systems still depend on developers, infrastructure providers, exchanges, or other centralized components.

The findings therefore support a broader interpretation of Web3 as an evolving ecosystem rather than a completed technological model. Blockchain can contribute to digital ownership, programmable coordination, and peer-to-peer interaction, but these capabilities do not eliminate conventional institutional requirements. Effective Web3 systems still require identity management, legal recognition, security controls, user protection, governance mechanisms, and reliable interfaces with the physical and institutional world.

3.5.3 Future Research Priorities and Adoption Pathways

The evidence synthesized in this review identifies several priorities for future blockchain research and adoption. First, greater attention is needed for scalable, interoperable, and governance-oriented architectures that can connect heterogeneous blockchain networks with conventional databases, cloud platforms, IoT devices, and organizational information systems. Future studies should move beyond laboratory demonstrations and evaluate whether blockchain solutions maintain acceptable performance, security, cost, usability, and governance characteristics under realistic workloads. Research on scalable data infrastructure and self-adaptive AI systems demonstrates the importance of reliable data management, system flexibility, and continuous performance evaluation in large-scale digital decision environments (Sami et al., 2024; Hossain et al., 2026).

Second, privacy-preserving blockchain technologies require further investigation. Approaches such as encryption, selective disclosure, zero-knowledge methods, secure data sharing, and off-chain storage may help protect sensitive information, but their adoption can introduce computational, usability, interoperability, and governance challenges. These issues are particularly important in healthcare, where data-driven systems are increasingly used for precision medicine, cancer treatment, health informatics, disease surveillance, and public-health decision-making (Hasan et al., 2026; Alam et al., 2025; Sami et al., 2026; Rahman et al., 2025). Future research should therefore evaluate privacy mechanisms not only by technical performance but also by regulatory compliance, organizational feasibility, cost, equity, and user trust.

Third, future blockchain research should examine sustainability and system efficiency using multidimensional measures. Evaluation should include energy requirements, hardware demands, transaction speed, scalability, security, decentralization, resilience, and governance. This broader approach is necessary because the sustainability of a digital system depends not only on electricity use but also on infrastructure design, operational efficiency, and the value created in practical applications. Research on IoT-enabled agro-food waste management, climate-resilient agritech, and smart-home systems illustrates how integrated digital technologies can support resource management and real-time decision-making when appropriately designed (Das et al., 2025; Alam et al., 2023; Habib et al., 2024).

Regulatory harmonization is another major priority. Cross-border blockchain applications require clearer approaches to data protection, digital assets, smart contracts, taxation, consumer protection, cybersecurity, and legal accountability. Comparative research across jurisdictions could identify areas of convergence and divergence while helping policymakers develop governance frameworks that support innovation without overlooking identifiable risks. This need is particularly relevant for consumer-facing applications, such as AI-driven e-commerce personalization, as well as high-consequence systems involving financial, health, industrial, and safety data (Alasa et al., 2025b; Sarwer et al., 2022).

Finally, the literature reveals a need for stronger empirical evidence from real-world implementation. Future research should use longitudinal case studies, comparative field research, mixed-method designs, and quantitative evaluations to assess user adoption, organizational performance, cost-effectiveness, security, governance outcomes, and social impacts. Blockchain applications should also be assessed in combination with AI, big-data analytics, IoT, cloud systems, and domain-specific models rather than as isolated technologies.

This integrated perspective is relevant across multiple sectors. In agriculture, blockchain-enabled systems could potentially support traceability and trusted data exchange for crop recommendation and production decisions (Alam et al., 2024; Alam et al., 2026). In healthcare and biotechnology, secure and auditable records may support collaboration in pharmaceutical development, disease surveillance, and clinical data management, although predictions and digital records must remain subject to biomedical and experimental validation (Tanvir et al., 2020; Rahman et al., 2022; Tanvir et al., 2024; Bulbul et al., 2019). In cybersecurity and mental-health applications, secure data handling and accountable system design are equally important because inaccurate or compromised information can create serious risks (Kaur et al., 2025; Ayrin et al., 2025).

Industrial and public-safety applications further show why implementation must be evidence based. Fire-protection, fire-dynamics, smoke-propagation, early-warning, and suppression research emphasizes that digital systems must be integrated with validated physical knowledge, safety procedures, and operational expertise (Hossain, 2021, 2022; Hossain et al., 2023; Hossain & Alasa, 2024a, 2024b; Hossain et al., 2024; Hossain, 2025). Similar considerations apply to hydrogen-related industrial processes, where secure, interoperable data systems may support traceability and operational coordination but must be evaluated within

real technical and regulatory conditions (Alasa et al., 2025a). Overall, the future adoption of blockchain will depend not on the technology alone, but on interoperable infrastructure, privacy-preserving design, sustainable technical models, clear governance, skilled personnel, and rigorous evidence from real-world deployment.

4. Conclusion

This systematic review demonstrates that blockchain technology has evolved substantially beyond its original association with cryptocurrency, emerging as a versatile infrastructure for improving transparency, traceability, security, decentralization, and trust across diverse sectors. The findings indicate significant applications in supply chain management, healthcare, financial services, public administration, education, energy, identity management, and digital rights, where blockchain can support secure data sharing, automated transactions, provenance verification, and more accountable institutional processes. At the same time, the review highlights persistent challenges, particularly scalability limitations, interoperability difficulties, regulatory uncertainty, privacy concerns, high implementation and energy costs, governance complexity, and shortages of technical expertise, which continue to constrain widespread adoption. Emerging developments, including interoperable blockchain networks, blockchain-as-a-service, smart contracts, decentralized identity, tokenization, and integration with artificial intelligence and the Internet of Things, suggest that future blockchain ecosystems are likely to become increasingly application-oriented and interconnected. Overall, blockchain should not be viewed simply as a cryptocurrency technology but as an evolving digital infrastructure whose long-term value will depend on addressing technical, organizational, regulatory, ethical, and environmental constraints while ensuring that implementations are aligned with clearly defined institutional and societal needs. Future research should therefore prioritize empirical evaluation of large-scale deployments, cross-sector interoperability, sustainable architectures, regulatory frameworks, privacy-preserving mechanisms, and the measurable long-term impacts of blockchain-enabled systems.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers

Artificial Intelligence (AI) Use Disclosure: The authors declare that no artificial intelligence tools were used in the preparation of this manuscript.

References

- [1] Abrar, I., & Sheikh, J. A. (2024). Current trends of blockchain technology: architecture, applications, challenges, and opportunities. *Discover Internet of Things*, 4(1), 7.
- [2] Aggarwal, S., Budhiraja, M., & Kataria, I. (2023). A systematic literature review on "financial technology (fintech): Trends, challenges, and future directions". *Journal of Global Information and Business Strategy*, 15(1), 75-83.
- [3] Alam, M. I., Hemal, M. A. K. P., Sami, M. A., & Rahman, M. L. (2024). Robust and interpretable crop recommendation. *European Journal of Ecology, Biology and Agriculture*, 1(5), 168-184. <https://doi.org/10.59324/ejeba.2024.1%285%29.14>.
- [4] Alam, M. I., Sami, M. A., Al Masud, A., Ahmed, H., & Hossain, F. (2025). AI-driven big data analytics for personalized cancer treatment. *Journal of Computer Science and Technology Studies*, 7(11), 428-441. <https://doi.org/10.32996/jcsts.2025.7.11.40>.
- [5] Alam, M. I., Sami, M. A., Hemal, M. A. K. P., & Rahman, M. L. (2023). Predictive analytics and decision intelligence for climate-resilient agritech systems, 2(1), 44-56. <https://doi.org/10.32996/agjcs.2023.2.1.4>.
- [6] Alam, M. I., Sikder, T. R., Sami, M. A., Rahman, M. L., et al. (2026). A robust and explainable approach to crop recommendation. *Journal of Environmental and Agricultural Studies*, 7(3), 1-15. <https://doi.org/10.32996/jeas.2026.7.3.1>.
- [7] Alasa, D. K., Hossain, D., Jiyane, G., Sarwer, M. H., & Saha, T. R. (2025b). AI-Driven Personalization in E-Commerce: The Case of Amazon and Shopify's Impact on Consumer Behavior. *Voice of the Publisher*, 11(1), 104-116. <https://doi.org/10.4236/vp.2025.111009>
- [8] Alasa, D.K., Hossain, D., Jiyane, G. (2025a). Hydrogen Economy in GTL: Exploring the role of hydrogen-rich GTL processes in advancing a hydrogen-based economy. *International Journal of Communication Networks and Information Security (IJCNIS)*, 17(1), 81-91. Retrieved from <https://www.ijcnis.org/index.php/ijcnis/article/view/8021>
- [9] Ayrin, F. J., Rahman, M. M., Quader, M. A., Dass, A., Khondaker, M. M. H., & Chakraborty, M. (2025). MentalLLM: A transformer-based large language model framework for depression detection. In 2025 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE). <https://doi.org/10.1109/WIECON-ECE69386.2025.11525902>
- [10] Bulbul, I. J., Zahir, Z., Ahmed, T., & Alam, P. (2019). Comparative study of the antimicrobial, minimum inhibitory concentrations (MIC), cytotoxic and antioxidant activity of methanolic extract of different parts of *Phyllanthus acidus* (L.) Skeels (family: Euphorbiaceae). *World Journal of Pharmacy and Pharmaceutical Sciences*, 8(1), 12-57. <https://doi.org/10.20959/wjpps20191-10735>
- [11] Das, K., Tanvir, A., Rani, S., & Aminuzzaman, F. M. (2025). Revolutionizing agro-food waste management: Real-time solutions through IoT and big data integration. *Voice of the Publisher*, 11(1), 17-36. <https://doi.org/10.4236/vp.2025.111003>
- [12] Gad, A. G., Mosa, D. T., Abualigah, L., & Abohany, A. A. (2022). Emerging trends in blockchain technology and applications: A review and outlook. *Journal of King Saud University Computer and Information Sciences*, 34(9), 6719-6742.
- [13] Habib, M. R., Yusuf, M. A., Warnasuriya, W. M. H. N., Sunny, K., Rahaman, M. M., & Khan, M. R. K. (2024). A comprehensive review on the advancement of home automation system. In 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) (pp. 638-642). IEEE. <https://doi.org/10.1109/ICoICI62503.2024.10696135>

- [14] Hasan, M. M., Alam, M. I., Chowdhury, M. A. H., & Anwar, M. M. (2026). AI-driven big data analytics for precision medicine and healthcare intelligence. *Frontiers in Computer Science and Artificial Intelligence*, 5(2), 41–62. <https://doi.org/10.32996/jcsts.2026.5.1.5>.
- [15] Hemal, M. A. K. P., Sayeed, N., Sami, M. A., Alam, M. I., Sikder, T. R., Dipa, S. A., & Rahman, M. L. (2025). Leveraging data analytics to strengthen public health and global economic sustainability. *European Journal of Medical and Health Research*, 3(4), 253–263. <https://doi.org/10.59324/ejmhr.2025.3%284%29.37>.
- [16] Hossain D., Alasa D.K, Jiyane G. (2023). Water-based fire suppression and structural fire protection: strategies for effective fire control. *International Journal of Communication Networks and Information Security (IJCNIS)*. 15(4):485-94. Available from: <https://ijcnis.org/index.php/ijcnis/article/view/7982>.
- [17] Hossain D., Alasa D.K. (2024a). Numerical modeling of fire growth and smoke propagation in enclosure. *Journal of Management World*. (5):186-96. <https://doi.org/10.53935/jomw.v2024i4.1051>.
- [18] Hossain D., Alasa D.K. (2024b). Fire detection in gas-to-liquids processing facilities: challenges and innovations in early warning systems. *International Journal of Biological, Physical and Chemical Studies*. 6(2):7-13. <https://doi.org/10.32996/ijbpcs.2024.6.2.2>.
- [19] Hossain, D. (2022). Fire dynamics and heat transfer: advances in flame spread analysis. *Open Access Res J Sci Technol*. 2022;6(2):70-5. <https://doi.org/10.53022/oarjst.2022.6.2.0061>.
- [20] Hossain, D. (2025). Water Efficient Suppression Material Fire Behaviour and AI Driven Safety in Future Fire Protection Research. *EJSMT*, 1(5), 62–76. [https://doi.org/10.59324/ejsmt.2025.1\(5\).07](https://doi.org/10.59324/ejsmt.2025.1(5).07)
- [21] Hossain, D.(2021). A fire protection life safety analysis of multipurpose building. Available from: https://digitalcommons.calpoly.edu/fpe_rpt/135/.
- [22] Hossain, D., Asrafuzzaman, M., Dash, S., & Rani, S. (2024). Multi-Scale Fire Dynamics Modeling: Integrating Predictive Algorithms for Synthetic Material Combustion in Compartment Fires. *Journal of Management World*. (5): 363-374.<https://doi.org/10.53935/jomw.v2024i4.1133>
- [23] Hossain, M. J., Bakhsh, M. M., Sami, M. A., Alam, M. I., Melon, M. M. H., & Manik, M. M. T. G. (2026). Self-adaptive artificial intelligence systems for large-scale data-driven decision making. In 2026 IEEE I3CTCON (pp. 1–8). <https://doi.org/10.1109/I3CTCON68242.2026.11507252>.
- [24] Islam, S., Khan, S. I., Ashik, A. A. M., Hossain, E., & Tanvir, A. (2025). Integrating data analytics into health informatics: Advancing equity, pharmaceutical outcomes, and public health decision-making. *Eurasian Journal of Medicine and Oncology*, 9(4), 284–295. <https://doi.org/10.36922/EJMO025300319>.
- [25] Kaur, J., Prabha, M., Samiun, M., Hasan, S. N., Hasan, R., Esa, H., et al. (2025). Comparative analysis of transformer and LSTM architectures for cybersecurity threat detection. *EAI Endorsed Transactions on AI and Robotics*, 4. <https://publications.eai.eu/index.php/airo/article/view/9759>.
- [26] Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. *Applied Sciences*, 11(20), 9372.
- [27] Le, T. V., & Hsu, C. L. (2021). A systematic literature review of blockchain technology: Security properties, applications and challenges. *Journal of Internet Technology*, 22(4), 789–802.
- [28] Miraz, M. H., & Ali, M. (2018). Applications of blockchain technology beyond cryptocurrency. arXiv preprint arXiv:1801.03528.
- [29] Nandanwar, H., & Katarya, R. (2023, March). A systematic literature review: approach toward blockchain future research trends. In 2023 International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT) (pp. 259-264). IEEE.
- [30] Ogayemi, A. (2026). From obligation to enforcement: mapping EU AI act and CRA cybersecurity requirements to technical controls for LLM-based autonomous agents. *International Journal of Information Security*, 25(5), 164.
- [31] Rahman, M. M., Juie, B. J. A., Tisha, N. T., & Tanvir, A. (2022). Harnessing predictive analytics and machine learning in drug discovery, disease surveillance, and fungal research. *Eurasia Journal of Science and Technology*, 4(2), 28-35. <https://doi.org/10.61784/ejst3099>.
- [32] Rahman, M. M., Rahman, M. S., Islam, S., Khan, S. I., Ashik, A. A. M., Hossain, E., & Tanvir, A. (2025). Integrating data analytics into health informatics: Advancing equity, pharmaceutical outcomes, and public health decision-making. *Eurasian Journal of Medicine and Oncology*, 9(4), 284–295. <https://doi.org/10.36922/EJMO025300319>
- [33] Romano, D., & Schmid, G. (2021). Beyond bitcoin: recent trends and perspectives in distributed ledger technology. *Cryptography*, 5(4), 36.
- [34] Sami, M. A., Hemal, M. A. K. P., Alam, M. I., & Rahman, M. L. (2024). Data governance and analytics infrastructure for scalable decision-making. *European Journal of Applied Science, Engineering and Technology*, 2(2), 388–403. <https://doi.org/10.59324/ejaset.2024.2%282%29.28>.
- [35] Sami, M. A., Rahman, M. L., Tanni, Z. A., Munmun, Z. S., Nusrat, S., & Biswas, B. (2026). Artificial intelligence and big data for precision medicine. *Frontiers in Computer Science and Artificial Intelligence*, 5(6), 36–43. <https://doi.org/10.32996/fcsai.2026.5.6.7>.
- [36] Sarwer, M. H., Saha, T. R., & Hossain, D. (2022). Driving Business Innovation with Artificial Intelligence, Machine Learning and Blockchain Technology. *Journal of Business and Management Studies*, 4(3), 221-230. <https://doi.org/10.32996/jbms.2022.4.3.21>
- [37] Sunny, F. A., Hajek, P., Munk, M., Abedin, M. Z., Satu, M. S., Efai, M. I. A., & Islam, M. J. (2022). A systematic review of blockchain applications. *Ieee Access*, 10, 59155-59177.
- [38] Tanvir A, Jo J, Park SM. Targeting Glucose Metabolism: A Novel Therapeutic Approach for Parkinson's Disease. *Cells*. 2024 Nov 13;13(22):1876. doi: 10.3390/cells13221876. PMID: 39594624; PMCID: PMC11592965.
- [39] Tanvir, A., Juie, B. J. A., Tisha, N. T., & Rahman, M. M. (2020). Synergizing big data and biotechnology for innovation in healthcare, pharmaceutical development, and fungal research. *International Journal of Biological, Physical and Chemical Studies*, 2(2), 23–32. <https://doi.org/10.32996/ijbpcs.2020.2.2.4>
- [40] Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. *Electronics*, 12(3), 546.
- [41] Yli-Huoma, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PLoS one*, 11(10), e0163477.