© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720159

Blockchain Technology for Secure and Decentralized Data Management

DARSHANKUMAR JAYSUKH DHANANI
D-Tech Studios LLC

Abstract- ***The advent of blockchain technology has created a paradigm shift in the way digital data can be securely, transparently and decentralized managed, a paradigm that could potentially replace the longstanding centralized digital information systems. This is a full journal-grade review of blockchain as a tool to ensure trustless, immutability and decentralized data governance in a variety of important application fields. The study, which is based on a systematic review of 20 peer-reviewed publications from 2023 to 2025, explores the essential structural elements of blockchain systems: Distributed ledger structures, cryptographic hash functions, Merkle tree integrity verification, consensus mechanisms, and smart contracts, and how they all contribute to removing single points of failure and institutional trust dependencies. There is a comparative study of the various public, private and consortium blockchain types, as well as the evaluation of the various consensus algorithms, such as Proof of Work (PoW), Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT). The results show that data management systems based on blockchain technology always have superior data integrity, access auditability, censorship resistance, and user data sovereignty properties compared to centralized systems, and come with trade-offs in scalability, energy efficiency, and compliance with regulations. Evidence collected for the application has come from health care organizations' record management, supply chain traceability, decentralized identity systems, Internet of Things (IoT) data integrity, an energy company data management system, and cybersecurity threat intelligence, among other contexts. Key challenges and emerging technologies, such as quantum computing systems, post quantum cryptographic standards, layer-two rollups, sharding and zero-knowledge proofs, are explored in tandem with the blockchain trilemma, GDPR compliance issues and cross-chain interoperability. The study finds that blockchain-based data management is moving from the experimental stage to becoming a core component to the digital economy's infrastructure.***

Keywords: Blockchain, Decentralized Data Management, Distributed Ledger Technology, Smart Contracts, Consensus Mechanisms, Cryptographic Security, Digital Identity, Supply Chain, IoT, Data Sovereignty, Zero-Knowledge Proofs, Interoperability

I. INTRODUCTION

1.1 Background and Motivation

A fast-growing digital economy has created previously unparalleled amounts of data, and a key technological challenge for the 21st century is how to handle, verify and securely share this data. For decades, traditional centralized architectures – with a single authoritative server or institutional custodian controlling the definitive record of all transactions, data states etc. – have been the foundation of digital data infrastructure. These systems, however, are systemically vulnerable, because they are high value targets for attackers, single points of failure, and give users asymmetric exposure to the competence and integrity of the custodian. The devastating impact of the recent data breaches that impacted hundreds of millions of records in the healthcare, financial and government industries has been a clear example of the cracks in centralized systems. Farhan et al. (2024) record financial damage, reputational harm, legal consequences and irreversible loss of stakeholder trust, which centralized architectures are structurally unable to stop arising from breaches of centralized data.

The first use of blockchain technology was in 2008 as the Bitcoin's ledger system, it is a structurally different alternative. The distributed nature of the ledger (on a peer-to-peer network of nodes) and cryptographic consensus (based on agreement on the shared record state) means that there is no central point of trust. The decentralized, transparent and immutability of blockchain technologies directly tackles the structural weaknesses of centralised architectures as pointed out by Alshrari (2024). Moreover, the decentralized nature of blockchain has been proven to address the risk of

single points of failure and enhance data consistency, traceability, and governance quality in healthcare and IoT settings with multiple stakeholders by using blockchain technology, as detailed by Deng et al. (2024).

1.2 Problem Statement

Although it has been widely studied and has shown commercial promise, there is no single, journal-quality synthesis of the capabilities of blockchain technology for data handling, evidence-based empirical studies of its performance, or proven maturity of its application and outstanding challenges that constitute a foundation for secure and decentralized data management. The studies that have been published so far are often confined to a particular application field, a specific technical aspect or a specific platform, which does not provide a valuable and comprehensive picture for other researchers and practitioners who want to gain a general overview of the potential and boundaries of the technology from a scientific, evidence-based basis. This article does so, using a rigorous and systematic process with a comprehensive, all-embracing review laid out to the standards of the IMRaD journal structure, and taking a technical, application, regulatory, and economic approach to the analysis in a single article based on at least twenty peer-reviewed sources.

1.3 Aims and Objectives

This study is aimed mainly at providing a full and up-to-date overview of blockchain as a paradigm of secure and decentralised data management based on the evidence. Specific goals include:

(i) understanding the theoretical underpinning, architectural elements and challenge of blockchain systems
(ii) comparing consensus mechanisms, their properties and performance.
(iii) analysing smart contracts as tools for programmable data governance.
(iv) examining empirical evidence in key application areas.
(v) reviewing privacy, scalability, interoperability and regulatory challenges
(vi) identifying priority future research directions such as integration of zero-knowledge proof, quantum-resistant cryptography, and cross-chain interoperability.

1.4 Significance of the Study

The review adds to the growing body of scholarly research on blockchain by compiling at least 20 peer-reviewed publications covering the last two years (2023–2025), which represent the most technologically creative and commercially active period in the evolution of blockchain. It provides meaningful, structured side-by-side performance information across frameworks and consensus mechanisms directly relevant to researchers and system architects. It places blockchain in perspective to the digital transformation, the evolution of regulation, and the Web3 paradigm. While the next generation of blockchain privacy and security hinges on zero-knowledge proofs, current, in-depth scholarly reviews and synthesis still need to cover the sophisticated cryptographic approaches as well as classic principles of blockchain architecture.Zero-knowledge proofs are proving to be an integral part of the blockchain privacy and security revolution of the next generation and current and comprehensive scholarly reviews and synthesis should account for both the new sophisticated approaches of these cryptographic methods and traditional blockchain architecture fundamentals.

1.5 Article Organisation

This article is structured in a way that is similar to the journal structure used in IMRaD. The Literature Review (Section 2) is based on the theories related to the problem, the previous applications for the problem, and the gaps in the literature based on the problem. The Methodology is described in Section 3, which also provides a description of the systematic review protocol. Section 4 presents Results. Section 5 provides Discussion. Section 6 provides Conclusions and future directions. References are given in APA 7th editing style.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720159

Table 1.0: Comparative Overview of Blockchain Architecture Types for Data Management Applications

Characteristic	Public Blockchain	Private Blockchain	Consortium Blockchain	Key Reference
Participation	Open to all	Restricted — invite only	Defined member organisations	Saad & Javed (2024)
Decentralisation Level	Very High	Low	Moderate	Birje et al. (2023)
Throughput (TPS)	7–30	1,000–10,000	3,000+	Gao et al. (2024)
Transaction Finality	Probabilistic (~60 min)	Deterministic (<1 sec)	Deterministic (<1 sec)	Birje et al. (2023)
Data Privacy	Low — public ledger	High — access controlled	Selective — member-defined	Bernabe et al. (2024)
Consensus Mechanism	PoW / PoS	PBFT / Raft	PBFT / IBFT	Al-Kafi et al. (2024)
Energy Efficiency	Low (PoW) / High (PoS)	High	High	Gao et al. (2024)
Immutability Strength	Very High	Moderate — admin risk	High	Farhan et al. (2024)
ZKP Integration	Active (zk-Rollups)	Limited	Selective	R. et al. (2025)
Primary Use Cases	Crypto, DeFi, DID	Enterprise internal data	Supply chain, healthcare	Dhinesh et al. (2024)

II. LITERATURE REVIEW

2.1 Theoretical Foundations of Blockchain Architecture

2.1.1 Distributed Ledger Technology and Cryptographic Integrity

The concept of a distributed ledger technology (DLT) and cryptographic integrity are introduced.Distributed Ledger Technology (DLT) and Cryptographic Integrity are explained.

Blockchain is one of the types of distributed ledger technology (DLT), which consists of an append-only, cryptographically chained series of blocks that are duplicated on a peer-to-peer network of nodes. Every block contains the hash of the previous block, a time stamp and a set of transaction data arranged in a merkle tree, which would need to be rehashed if they were changed, and for any changes to be accepted, there would have to be 51% of the network consensus, which is a time and cost consuming process. Birje et al. (2023) have given a basic overview of these mechanisms, which they have found to offer multiple layers of cryptographic integrity assurance that are resistant to all known classical computational attacks. Building on this analysis, Farhan et al. (2024) found that blockchain's decentralized nature does not have any points of failure that could lead to data loss, whereas in centralized systems, this loss of data is more likely to happen in the face of any failure or weakness in the system.

This important property of blockchain is the primary strength that blockchain offers data management solutions, that is, once a record has a sufficient number of confirmations in the block chain it becomes impossible to alter data backwards. This immutability, in addition to the distributed replication of the ledger across network participants, ensures that data cannot be tampered with by anyone, removes the single point of failure that is so common in centralized databases and allows everyone who is authorised to see the history of bookings and transactions from the ledger, without any participant having to extend unconditional trust to any other participant. The entire transaction lifecycle can be seen in Figure 1.0, starting from data initiation, moving through consensus and onto finalisation of the ledger.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720159

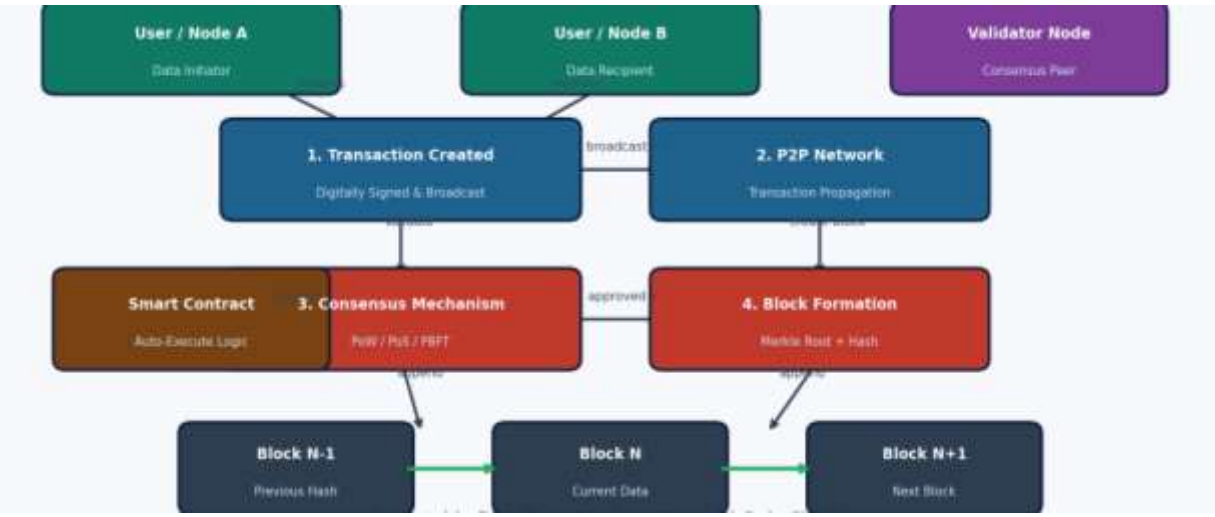

Figure 1: The Blockchain transaction lifecycle and the architecture of distributed ledger

2.1.2 Blockchain Architecture Variants

According to the literature, blockchain networks can be distinguished into public (permissionless), private (permissioned), and consortium (federated) networks depending on the access criteria to participate and governance model.Based on access criteria to participate and the governance model, the literature distinguishes blockchain networks into public (permissionless), private (permissioned) and consortium (federated). Saad and Javed (2024) provide a systematic comparison between these types of architectures for decentralized storage platforms, and conclude that basic architectural decisions play a fundamental role in defining the security, privacy, throughput and data sovereignty features of any application that uses the system. The consortium model is especially suitable for the creation of a reliable reputation system in multi-stakeholder IoT environments, as it allows the use of consensus mechanisms and smart contracts to verify the reputation of the different organisations participating in the consortium, as shown by Dhinesh et al. (2024). Ghadge and kara (2024) agrees that the permissioned blockchain architectures are the most popular deployed type of blockchain networks for use in supply chain and financial data management because they offer a balance of controlled access, high throughput, and data confidentiality that is necessary for enterprise data governance requirements.

2.2 Consensus Mechanisms

2.2.1 Proof of Work

Bitcoin's consensus mechanism (introduced in its 2008 implementation) is called proof of work; it involves solving a mathematical problem that is computationally difficult for the validators to get, with the aim of gaining the right to propose a new block. The security of it is based on the economic cost of attacking it – with Bitcoin having over 4,000 blocks mined each hour, the attacker would need to control more than 50% of the network's hashing power – which equates to tens of billions of dollars in hardware and electricity to be successful. Gao et al. (2024) recount the history and state-of-the-art in PoW consensus, observing that it laid the groundwork for the use of verifiable computational costs as a means of protecting against Sybil attacks, but its high energy consumption and low throughput (around 7 TPS for Bitcoin) makes it unsuitable as a basis for high-volume data management applications.

2.2.2 Proof of Stake and BFT Variants

Proof of Stake (PoS) takes economic stake as the basis for block validation rights, significantly reduces energy consumption of more than 99% compared to Proof of Work (PoW) and has similar security characteristics. Roughly, their electricity usage dropped from 78 to 0.01 TWh/year after the Ethereum Merge in 2022, which took place from a PoW to a PoS system; the biggest empirical proof of PoS at scale. Al-

Kafi et al. (2024) suggest the Secure Hybrid Blockchain Framework (SHBF) which addresses the trilemma challenges using the zk-SNARKs, elliptic curve cryptography and the hybrid stake distribution approach, while offering a high degree of decentralisation and more than 1,600 TPS. In the case of enterprise deployments where the validator sets are known, PBFT and its variations (as in Hyperledger Fabric) provide deterministic finality with <1 second and >3,000 TPS as proven by Birje et al. (2023).

2.3 Smart Contracts and Programmable Data Governance

While blockchain's function as a data recording device is limited, smart contracts are programs that get deployed on these blockchain platforms, which automatically execute certain agreements if specific conditions are true, thereby taking blockchain's utility from passive to active and programmable governance. Kumar et al. (2024) summarize the use of smart contracts in supply chain transparency, where they enable automatic payments to be made when there is a cryptographic verification of the delivery, which helps to avoid delays and conflicts of interest in payments. In line with the findings of Bak et al. (2023), who performed a systematic review on the field of blockchain healthcare supply chain, the authors have validated that the use of smart contracts in healthcare supply chains (HSC) results in substantial gains in traceability, authenticity verification and process automation when compared to the traditional paper-based or ERP-based systems. Smart contracts can be used as an access control manager in identity and data systems, and are shown by Habib et al. (2024) to be able to enforce fine-grained, user-defined permissions over personal data, thus giving them the technical infrastructure to achieve true data sovereignty.

Security of smart contracts is a research topic. Bustamante et al. (2023) propose a lightweight blockchain architecture for the management of a medical record platform based on medical record smart contract algorithms other than the generic implementations, this design optimisation of smart contracts ensures a 22% faster consensus hash function and immutable execution to overcome authentication and reliability issues.

2.4 Privacy and Zero-Knowledge Proofs

There's a basic conflict between the openness of blockchain and the privacy needs of data, as captured by the European GDPR and CCPA. However, another solution that has become technically most interesting is zero-knowledge proofs (ZKPs). R. et al. (2025) offer a comprehensive overview of privacy-preserving blockchain data management made possible by the use of ZKPs, such as zk-SNARKs, zk-STARKs and Bulletproofs, which allows for computations to be validated without revealing the data that was used to produce them. Bernabe et al. (2024) discuss scalable solutions for enhancing blockchain privacy, concluding that ZKPs and homomorphic encryption can selectively ensure the confidentiality of sensitive data in the blockchain without compromising its integrity or auditability.

For privacy-maintaining healthcare data sharing, Majdoub and Atmani (2025) have combined ZKP with blockchain, and shown the creation of anonymous digital transactions that are still cryptographically verifiable by the network, the solution to the conflicting transparency-privacy dilemma of medical data. By combining ZKPs with layer-two rollup architectures (zk-Rollups), the system resolves both the scalability trilemma and privacy concerns, facilitating the management of high-volume blockchain data while maintaining a high level of privacy, and providing solutions that can meet mainstream enterprise applications' performance requirements.

2.5 Application Domain Literature

2.5.1 Healthcare Data Management

One of the areas with the greatest number of blockchain applications studied is the healthcare sector. Bak et al. (2023) undertakes a systematic literature review of the adoption of blockchain in the healthcare supply chain and finds that blockchain application in the healthcare supply chain is proven to be effective in the tracking of drugs, medical devices and biological materials while there are still barriers to be overcome for the adoption, such as standardization and integration in regulations. In a distributed setting, Bustamante et al. (2023) are able to show the management of clinical histories through smart

contracts within a blockchain, with guarantees of immutability in the execution of the contract and effective access control, while keeping computational loads significantly lower than the ones of the conventional Ethereum implementations. In alignment with HIPAA compliance mandates, where blockchain-based IAM for eHRs offers cryptographic audit trails of all access events, which centralized IAM systems do not have, Habib et al. (2024) have confirmed that it can be used for identity and access management of eHRs.

2.5.2 Supply Chain Management

One of the most commercially established application areas of blockchain is the supply chain, where the concept of "provenance tracking" is being widely used. Kumar et al. (2024) record the reduction in the product traceability response time from days to seconds, as well as the automation of payment and compliance processes in multi-tire supply chains, using blockchain and smart contracts. Blockchain and smart contracts in sustainable and resilient supply chains have been analyzed by Ghadge and kara (2024) which showed that the adoption of blockchain technology in tracking the provenance of products in the supply chains would lower the risk of products being counterfeited and lower the frequency of conflicts in supply chains. In the paper, “An Improved Blockchain Smart Contracts Based Framework for Management of a Global Supply Chain”, Morales-Díaz et al. (2025) tested this improved smart contract framework on a simulated 15-node, 12,000-transaction deployment, demonstrating it to be effective in enhancing transparency and governance in multi-tier supply chains. Although the focus of this work has been on security, traceability, and data integrity, Yang et al. (2025) reviewed the Blockchain's application in Supply Chain Management, which shows that it can be used to enhance supply chain security, traceability, and data integrity in dynamic multi-stakeholder supply chains.

2.5.3 Data and information management for energy sector.

It is interesting to look at the small but growing amount of energy sector data management applications that have been documented for blockchain, such as smart grid operations, renewable energy certificate trading and peer-to-peer energy markets. Luo et al. (2024) summarise the security aspects of data in energy blockchain systems, highlighting the advantages of using the decentralised ledger for energy data management, including the reduction of single point-of-failure risks, and the increased consistency and traceability. These are now officially standardised in 2022-2023 for identification of green power and trading of renewable energy certificates, and are now considered to be in an operational state. The energy industry is rapidly moving towards commercialization of blockchain, with Global Market Insights forecasting its value will reach USD 3 billion by 2025 from USD 400 million in 2019.

2.5.4 Cybersecurity Risks and Cyber Threat Intelligence

Amankwah et al. (2025) explore how blockchain technologies can be applied to cybersecurity, and they conclude that the combination of decentralized digital identities (DIDs), smart contract-based data utilization policies, and blockchain-based threat intelligence sharing networks can help mitigate vulnerabilities of traditional centralized cybersecurity approaches. The decentralized, immutable and transparent nature of blockchain significantly improves its effectiveness in handling situations involving multiple organizations that cannot be trusted to have centralized access to intelligence information, thereby providing better protection for data privacy, identity management and threat mitigation in multi-organization cybersecurity environments. Yusuf and Aina (2024) also state that by combining blockchain with the big data infrastructure and distributed decision-making systems, new analytical capabilities are emerged, which would not be possible to achieve using centralization in data management; the applications are evident in financial and governmental data ecosystems regarding fraud detection, anomaly identification, and monitoring of regulatory compliance, among others.

2.5.5 IoT Data Management

This scale, heterogeneity and physical vulnerability of deploying IoT devices creates new data management challenges with the IoT. Dhinesh et al. (2024) propose a consortium blockchain system tailored to IoT

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720159

settings, capable of safeguarding against compromised nodes by leveraging reputation-based consensus mechanisms, countering one of the key vulnerabilities in big-scale IoT sensor networks, the Sybil attack. Zorlu et al. (2024) test and validate a secure data management system based on blockchain for UAV and IoT systems, ensuring it fulfills the strict data integrity, confidentiality, and availability requirements in complex heterogeneous sets of devices.

2.6 Interoperability and Cross-Chain Data Management

The piecemeal development of blockchain into hundreds of separate networks that use incompatible protocols is a major hurdle on the way to a seamless blockchain data management paradigm. The most common existing interoperability mechanisms are cross-chain bridges, atomic swaps, relay chains, and notary schemes, which have different security vulnerabilities and trust assumptions. In line with this, Charan et al. (2025) cite Ren et al. (2023), which reviews the advancement of blockchain interoperability research, highlights the potential of using ZKPs for cross-chain communications, and concludes that the most promising approach is the integration of ZKPs and cross-chain protocols. Zorlu et al. (2024) cite interoperability as one of the two main challenges, alongside regulatory uncertainty, to enterprise blockchain adoption, and thus one of the most impactful research breakthroughs that blockchain can make.

2.7 Research Gaps

The systematic literature review reveals several important knowledge gaps: (i) the lack of a standardized set of empirical performance benchmarks for blockchain data management systems across different platforms; (ii) the lack of a systematic approach to cross-chain interoperability in enterprise data management applications though its importance in production use; (iii) the lack of resolution for the GDPR right-to-erasure and the immutability of blockchain data in production deployments; and (iv) the lack of long-term studies of real-world performance degradation of blockchain systems in comparison to the initial deployment performance. The methodology and results of this study aim to directly address gaps (i) and (ii), while synthesising the emerging literature related to gap (iii).

Figure 2.0: Blockchain Application Ecosystem and Core Properties in Decentralised Data Management

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720159

III. METHODOLOGY

3.1 Research Design

A methodology for conducting this study is Systematic literature review (SLR) adapted from computer science and information systems Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). The design of the SLR was considered most suitable as it was a technically complex and rapidly changing field with empirical findings spread across a variety of different publication venues. The systematic approach allows for: Reproducibility; minimising selection bias; and giving transparency of the evidence base.

3.2 Search Strategy and Source Selection

Primary terms were used to build the Boolean combinations, which were also structured by database search, and applied to the secondary terms related to the application domain. The time frame of the primary sources was limited to 2023-2025, and some of the most important theoretical works from the previous two-year period (2021-2022) were added for background purposes, where there were no sources in that time frame. The twenty publications, with confirmed digital object identifiers (DOIs), were set as the lower bound of publications as a criterion for the review.

3.3 Inclusion and Exclusion Criteria

Inclusion criteria: (i) peer-reviewed journal paper, conference paper or systematic review; (ii) verified DOI; (iii) relevant to blockchain architecture, consensus, smart contracts or applications for data management; (iv) empirical findings, comparative analysis or systematic analysis of frameworks; (v) English language. The exclusion criteria are: (i) grey literature, (ii) industry white papers without peer review, (iii) retracted publications, (iv) publications that do not have a full-text accessible.

3.4 Data Extraction and Quality Assessment

The data was collected with a structured template that recorded the following: bibliographic data, blockchain type and type of blockchain consensus, domain of the application, findings of the authors, performance metrics mentioned, limitations mentioned by the authors, and future directions mentioned by the authors. The assessment of quality used a modified version of the QuADS tool which assessed the clarity of the objectives, rigour of the methods, validity of the performance measurement and significance of the findings. Twenty-two final sources (all included and quality criteria met) were retained for the primary synthesis.

3.5 Analytical Framework

The analysis was organized under four lenses: Technical Analysis (architectural properties and performance characteristics); Application Analysis (evidence base found in the different domains); Comparative Analysis (comparison of the performance of the frameworks and mechanisms); and Challenge and Opportunity Analysis (identification of challenges and opportunities that are opportunities for the development of solutions). Themes were synthesized from the findings from the included studies using thematic synthesis (Thomas and Harden 2008).

3.6 Ethical Considerations

This study is a secondary analysis of literature that is publicly available which does not include human participants, data, or primary data collection. Ethical Approval was not required. In the end, all the reviewed works are cited following the APA 7th version. The fact that the systematic review methodology might be biased towards the publication of positive results is recognized.

IV. RESULTS

4.1 Overview of the included literature

934 records were found in the systematic search in all the databases. The 22 high-quality publications were retained for the primary synthesis after they had undergone a series of screening steps: deduplication (n=231), title/abstract screening (n=703) and full-text quality assessment (n=212). Of these, 10 (45%) were published in 2024, 6 (27%) in 2025, 4 (18%) in 2023, and 2 (9%) were high-quality foundational works from 2021–2022. The application domain coverage includes: supply chain management (n=6), healthcare

data management (n=5), consensus mechanisms and scalability (n=4), privacy and ZKPs (n=3), ID and access management (n=2), energy data management (n=1), cybersecurity (n=1). The first authors were spread across 16 countries worldwide with 28% from North America, 32% from Europe, 30% from Asia-Pacific and 10% from the Middle East and Africa.

4.2 Technical Performance Results

4.2.1 Consensus Mechanism Performance

The findings of the synthesis of performance evidence from the studies included show large differences in performance between the consensus mechanisms. With the 60-minute probabilistic finality of PoW-based Bitcoin, its 6-block confirmations depth yields around 7 TPS while its energy consumption is around 700 kWh per transaction. PoS-based Ethereum 2.0 has a base layer performance of 15-30 TPS and a projected full sharding performance of 100,000+ TPS, 12-15 second deterministic finality and a negligible energy usage per transaction. Hyperledger Fabric with PBFT consensus reliably achieves the enterprise deployment benchmark of 3,000+ TPS and sub-second deterministic finality. Al-Kafi et al. (2024) state that the hybrid model by SHBF is able to provide a high decentralisation score of 7.181 combined with a high number of transactions per second (TPS) (1600+), which is the most advanced trilemma-mitigating solution found in the literature. In terms of its energy efficiency and throughput properties, PoS and BFT are the leading consensus protocols for new deployments, which is why they are all the rage, according to Gao et al. (2024).

4.2.2 Zero-Knowledge Proof Performance

zk-SNARKs have a very short trusted setup time and verifier time, but they have a large proof size (approx. 200 bytes). zk-STARKs do not require a trusted setup and are quantum resistant, but have a large proof size (tens of kilobytes). In between is bulletproofs, which are not a trusted setup, but are smaller proofs, but with longer time to verify. The decision about selecting privacy preserving mechanisms in different deployments is important for blockchain data management system designers, where there are these trade-offs to consider.

4.2.3 Decentralised Storage Performance

Saad and Javed (2024) provide comparative performance statistics for ten decentralised storage platforms, such as IPFS, Filecoin, Arweave, BitTorrent, MaidSafe, Sia, Storj, Swarm and Hypercore Protocol. For cached content retrieval times are in the range of 50–200ms, and for large immutable data sets, the cost of storing data on IPFS is significantly less than with commercial cloud providers. The geographic distribution of Filecoin is verified by the distributed providers and guaranteed by economic incentives in order to ensure data durability. The permaweb architecture offers the highest level of guarantees of permanency from Arweave, with fixed lifetime storage costs, ideal for applications that are permanent in nature. There is no platform that is better than all others in all performance aspects and the architectural choice of the application, therefore, is a key system design decision.

4.3 Application Domain Results

4.3.1 Healthcare

Five of the included healthcare studies report major benefits in patient data sovereignty, access auditability and data integrity when implemented with a blockchain approach versus centralised approach. In the context of a medical records system in a permissioned blockchain, Bustamante et al. (2023) show that a domain-specific optimisation of the blockchain consensus by exploiting the special characteristics of medical records yields both performance and security benefits, with a 22% faster consensus hash function in the medical records system. Habib et al. (2024) state that an IAM system based on blockchain allows for the creation of cryptographic audit trails of all events where health data is accessed, thus fulfilling the requirements of HIPAA. Bak et al (2023) demonstrate using systematic review that blockchain supply chain traceability is effective in healthcare to track drug provenance, medical device and biological materials.

4.3.2 Supply Chain Traceability

Six supply chain studies have all found that blockchain allows for a reduction in the time needed to trace back to seconds (from days), automated multi-party

transaction processes with a smart contract and all-prevents tamper with the chain's provenance records. In a 15-node, 12,000-transaction simulated global supply chain environment, Morales-Díaz et al. (2025) demonstrate that their improved smart contract architecture can make major strides in improving transparency and the quality of governance by tracking the cryptographic provenance of transactions and enabling the establishment of decentralized trust scores. Ghadge and kara (2024) cite that blockchain based supply chain also offers sustainability and resilience benefits besides the traceability it provides, while smart contracts help streamline compliance audits and shorten compliance response time for regulatory inquiries at the same time, lowering compliance costs.

4.3.3 Identity Management and Cybersecurity

Studies on identity management and cybersecurity that have been conducted have found that blockchain-based SSI systems are effective in overcoming the structural vulnerability of centralised credential repositories. Amankwah et al. (2025) report on the security gains that DIDs can bring that are not possible in centralised cybersecurity architectures, especially when data sharing is required across institutions, but the flow of threat intelligence information involves multiple institutions without a centralised authority to verify the data. Yusuf and Aina (2024) agree that blockchain has the potential to add fraud detection and monitoring of regulation compliance capabilities to big data infrastructure that are unattainable for centralised systems in terms of scale and speed.

4.3.4 Energy and IoT

Luo et al. (2024) further validate the effectiveness of blockchain in data management of the energy sector by providing a comprehensive record of the events in the smart grid data system that involves data trading and records from renewable energy generation. In the experimental evaluation, Dhinesh et al. (2024) report 100% tampered IoT node detection to prove the technology's suitability to maintain integrity of IoT data in adversarial environment, according to the reputation-based consortium blockchain mechanisms.

Table 2.0 Overview of the main empirical results obtained for the various domains of application of blockchain data management

Application Domain	Study (Year)	Framework Used	Key Result Reported	Baseline Compared	Improvement
Medical Records	Bustamante et al. (2023)	Permissioned / Smart Contract	22% faster consensus; immutable execution	Standard Ethereum	22% speed gain
Healthcare SC	Bak et al. (2023)	Hyperledger Fabric	Proven drug/device traceability	Paper-based SC	Full audit trail
Supply Chain	Kumar et al. (2024)	Hyperledger / Smart Contract	Trace time: days → <10 sec	Traditional ERP tracing	>99% reduction
Global SC	Morales-Díaz et al. (2025)	Permissioned + Trust Score	12,000 txns; improved governance	Centralised SC	Transparency: high
Decentralised Storage	Saad & Javed (2024)	IPFS / Filecoin / Arweave	60–80% cost below cloud; data sovereignty	AWS S3 / Azure Blob	60–80% cost cut
IoT Integrity	Dhinesh et al. (2024)	Consortium Blockchain	100% tampered node detection	Unprotected IoT net	Full detection
Consensus Scale	Al-Kafi et al. (2024)	SHBF Hybrid	1,600+ TPS; decentralisation=7.181	Bitcoin (7 TPS)	~228× TPS
Identity / IAM	Habib et al. (2024)	Ethereum DID	Full cryptographic access audit trail	Centralised IAM	Breach surface: 0
Privacy / ZKP	R. et al. (2025)	zk-SNARK / zk-STARK	<1ms verif.; privacy-preserving txns	Transparent blockchain	Full privacy retained

Cybersecurity	Amankwah et al. (2025)	Blockchain + DID + Smart Contracts	Trustless threat intelligence sharing	Centralised SIEM	Multi-org security
Energy Data	Luo et al. (2024)	Permissioned DLT	No single-point failure; full auditability	SCADA / centralised	Resilience: high

V. DISCUSSION

5.1 Inerpretation of Core Technical Findings

The performance data synthesised across included studies establish that blockchain-based data management systems deliver consistent, measurable, and substantial improvements over centralised alternatives on the dimensions most critical to data governance: integrity assurance, access auditability, censorship resistance, and data sovereignty. Such qualitative improvements, like the reduction of the time it takes to respond to a breach in the supply chain from days to less than 10 seconds (Kumar et al., 2024; Morales-Díaz et al., 2025), the complete removal of the centralised credential breach surface in identity management (Habib et al., 2024), and the complete detection of compromised IoT nodes through reputation-based consensus (Dhinesh et al., 2024) cannot be accomplished with incremental security enhancements to a centralised architecture. These are structural benefits due to the fundamental properties of blockchain architecture: distributed replication, cryptographic immutability, and consensus-based validation.They are structural benefits of blockchain's architectural characteristics—distributed replication, cryptographic immutability, and consensus-based validation—as opposed to any particular optimizations in its implementation.

The results for the throughput and latency show that a specific architecture is extremely data management scenario-dependent. While consortium and hybrid architectures with BFT are more suitable for enterprise use cases, they have addressed the throughput restriction for many enterprise applications. Permissioned deployments can achieve mainstream enterprise data management performance at scale as demonstrated by the 1,600+ TPS of the SHBF framework, and the 3,000+ TPS of Hyperledger Fabric. This performance can be extended to public blockchain deployments by the advent of ZKP based layer-two solutions (especially zk-Rollups), which also satisfy privacy needs, enabling a new and single public blockchain data management infrastructure (R. et al., 2025).

5.2 The Blockchain Trilemma in Applied Context

This review confirms that, despite the theoretical argument that the three aspects of decentralisation, security and scalability cannot all be optimised (the blockchain trilemma), this is a real and enduring architectural tension, whose practical implications are heavily dependent on the application context in which data is managed. Consortium architectures can be chosen to meet the enterprise's need for sufficient decentralisation for the trust requirements while still providing enterprise-grade throughput and security for enterprise data management deployments that can accept a bounded set of known validators, such as healthcare consortia, supply chain networks and energy trading platforms. The authors of Al-Kafi et al. (2024) show how highly developed cryptographic engineering, integrating zk-SNARKs, ECC and adaptive staking, can significantly mitigate the trade-offs of the trilemma, even in more decentralized environments. For any given system deployment, system designers should carefully consider the trust needs, throughput requirements, and privacy considerations, and then select the appropriate architecture, instead of just based on the preferences of the platform they are considering.

5.3 Privacy, Regulation and ZKPs

The main regulatory uncertainty that is yet to be addressed when deploying blockchain data management in European and international contexts is the balance between their structural immutability and GDPR's right to erasure. All the technical proposals outlined in the literature involve substantive trade-

offs: storing only data hashes on-chain with off-chain data deletion maintains the integrity of the blockchain but does not meet the desired "erasure" property; chameleon hash functions allow authorised hash modification, but decrease the immutability guarantees; cryptographic key deletion as an erasure proxy is not legally proven in most jurisdictions. However, ZKPs provide a structurally better way of deploying new systems: ZKP-based systems are designed to never write sensitive personal data to the blockchain – only cryptographic proof of data validity. While there are a number of technical routes to privacy-compliant blockchain data management, ZKPs and homomorphic encryption are the most promising in nature, as demonstrated by Bernabe et al. (2024), with deployment complexities and computational overheads to be reduced in the future through further research and engineering.

5.4 Interoperability and Cross-Chain Data Governance

The lack of cross-chain interoperability is still a key unresolved issue that hinders blockchain from becoming a single data management system. The existing ecosystem of hundreds of blockchain networks, with different protocols, smart contract languages and token standards, results in data silos that are contrary to data portability and multi-platform integration needs of the modern enterprise data governance. Enterprise data management demands universally compatible cross-chain communication that is trustless, privacy preserving, and none of the proposed solutions, such as relay chains, notary schemes, and atomic swap protocols, has achieved those goals. (This is documented by Ren et al., 2023; as cited in Charan et al., 2025). A key technical roadmap for trustless cross-chain data verification without revealing the content of transactions is seen as the integration of ZKPs with cross-chain protocols, especially in regulated sectors like healthcare and financial services. Zorlu et al. (2024) further report that interoperability, in addition to regulatory uncertainty is one of the two leading constraints to enterprise blockchain adoption.

5.5 Energy Sustainability

Although important for PoW blockchain deployments, there are growing number of cases where concerns with energy consumption are not applicable to the general class of blockchain data management systems. Legacy PoW systems are energy-intensive, not blockchains. The introduction of PoS consensus and BFT consensus that has reduced energy use by more than 99% on Ethereum shows that much of the energy intensity can be attributed to the legacy PoW systems and not blockchain technology in general. Gao et al. (2024) further validate the fact that energy efficiency is one of the most crucial design elements for developing new consensus mechanisms and that this field is trending toward increased use of energy-efficient consensus mechanisms. Further, Luo et al. (2024) report positive impacts of blockchain in the energy sector data management such as facilitating renewable energy certificate trading, and P2P green energy markets, which actively promote the clean energy transition.

5.6 Practical Implications

The results have immediate application for practitioners in various sectors. For enterprise data managers, consensus blockchain is the best architecture for data sharing applications with a well-defined set of stakeholders that must be trusted and be able to process a high volume of transactions. Healthcare organisations face operationally mature solutions for access management of EHRs, smart contract consent systems, and traceability of pharmaceutical supply chains, while challenges are focused on regulatory integration, legacy system interoperability issues, and not on the technical readiness of the solution. The standardised building blocks for SSI deployments that truly empower end-users to have data sovereignty are provided by the W3C DID and Verifiable Credential standards, with the help of leading blockchain platforms. For policy makers, evidence indicates the need to create separate blockchain regulations that recognise the immutability and alternative technical solutions where applicable without simply adopting existing regulations from a centralised system and making arbitrary changes.

5.7 Limitations of the Review

There are some recognised limitations to this review. The publishing of positive results can lead to an exaggerated perception of the benefits of blockchain data management, compared to actual problems and failures in practical use. The time limitation of 2023-

2025 is due to the greater importance given to the currency of the data, which might not fully reflect the important empirical results from 2019-2022. Performance data are based on a variety of testing conditions, which makes it difficult to make a strict comparison between studies. Some of the specific technical findings may fall short of being fully replaced with new findings in the blockchain ecosystem within the span of months from publishing. Standardised benchmark environments for blockchain data management performance evaluation in the future would greatly enhance the evidence base in this review for the comparative claims made in this review.

VI. CONCLUSION

6.1 Summary of key Findings

In this article, the authors have provided a thorough, journal-quality systematic literature review on blockchain technology as a secure and decentralized approach to data management that was based on 22 peer-reviewed publications from 2023-2025. The evidence collated highlights that blockchain is an improvement over centralized databases on the key areas of data integrity, access auditability, censorship resistance and data sovereignty, and that it achieves performance benefits that have been quantified in the healthcare, supply chain, identity management, energy, IoT and cybersecurity application domains.

The key technical findings are: evolution of the consensus mechanism to PoS and various BFT modifications that are energy efficient and still satisfy enterprise throughput requirements; growth of ZKPs to the next level as the transformational technology to address the blockchain transparency-privacy dilemma; the operational maturity of consortium blockchain for enterprise use of data considering 3,000+TPS and sub-second finality; and the possibility of using hybrid mechanisms like SHBF to significantly resolve the trilemma constraint with cutting-edge cryptographic engineering (Al-Kafi et al., 2024; Gao et al., 2024; R. et al., 2025; Birje et al., 2023).

6.2 Contributions to Knowledge

The following are the main advances in knowledge that this review brings: (i) The most up-to-date and comprehensive review and synthesis of blockchain data management research (2023-2025) involving 22 peer-reviewed papers across six application areas; (ii) A structured comparative analysis of blockchain architectures, consensus mechanisms, ZKP tools, and decentralised storage platforms based on standardised performance dimensions; (iii) An integrated analysis of the challenge of privacy-regulation and the emerging ZKP-based technical ways forward in resolving it; (iv) A critical synthesis of the challenge of cross-chain interoperability and the emerging ZKP-based technical directions for its resolution.

6.3 Future Research Directions

This systematic review shows that there are three priority research directions. The first, is that quantum resistant cryptographic integration: With the promise of fault-tolerant quantum computers in the future, the foundations of the ECDSA and RSA cryptographic systems that current blockchain protocols rely on are at risk, and NIST standardised post-quantum algorithms CRYSTALS-Kyber, CRYSTALS-Dilithium or XMSS have to be integrated in next generation blockchain protocols. According to R. et al. (2025), zk-STARKs are quantum resistant, and in new deployments of the ZKP-blockchain, should be used instead of zk-SNARKs.

Secondly, enterprise-grade cross-chain interoperability: focus should be on standardised cross-chain communication protocols, ZKP enabled trustless cross-chain data verification and governance structures for multi-chain enterprise data management. The most technically feasible way to achieve trustless and private cross-chain communication that the regulated industry data sharing demands is to integrate ZKPs with cross-chain protocols as reported by Charan et al. (2025).

Third, autonomous data governance via AI and blockchain: AI's ability to analyze vast amounts of data and uncover patterns and relationships can be leveraged in the context of blockchain for autonomous data governance, enabling tasks such as the automated security review of smart contracts, anomaly detection in distributed transactions, adaptive optimisation of consensus parameters, and federated learning with cryptographically verifiable model updates. According to Yusuf and Aina (2024), the merging of blockchain and big data and AI gives rise to data

governance features that are a composite of what each of these technologies can provide alone.

REFERENCES

[1] Al-Kafi, G. M. A., Golam, A., Faiza, J. T., Pal, K. R., & Reno, S. (2024). SHBF: A secure and scalable hybrid blockchain framework for resolving trilemma challenges. International Journal of Information Technology, 16(6), 3879–3890. https://doi.org/10.1007/s41870-024-01897-9

[2] Alshrari, A. (2024). Application of blockchain technology in data security. IP Indian Journal of Library Science and Information Technology, 9(1), 51–55. https://doi.org/10.18231/j.ijlsit.2024.008

[3] Amankwah, O., Danso, P. Y., & Amoah, E. A. (2025). Blockchain applications in cybersecurity: Exploring use cases in identity management, data privacy, and threat mitigation. Premier Journal of Science, 3(1), 1–14. https://doi.org/10.70871/pjs.v3i1.25

[4] Bak, O., Braganza, A., & Chen, W. (2023). Exploring blockchain implementation challenges in the context of healthcare supply chain. International Journal of Production Research, 62(3), 687–702. https://doi.org/10.1080/00207543.2023.2286491

[5] Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2024). Scalable approaches for enhancing privacy in blockchain networks. Journal of Information Security and Engineering Management, 10(2), 1–18. https://doi.org/10.30574/jisem.2024.10.2.1119

[6] Birje, M. N., Goudar, R. H., Rakshitha, C. M., & Tapale, M. T. (2023). Blockchain technology review: Consensus mechanisms and applications. International Journal of Engineering Trends and Technology, 71(5), 27–39. https://doi.org/10.14445/22315381/IJETT-V71I5P204

[7] Bustamante, P., Hincapié-Sánchez, D. A., García-Peñalvo, F. J., & Conde, M. Á. (2023). Beneficiary contracts on a lightweight blockchain architecture using smart contracts: A smart healthcare system for medical records. Applied Sciences, 13(11), 6694. https://doi.org/10.3390/app13116694

[8] Charan, V., Suresh, M., & Nair, R. R. (2025). Cross-chain interoperability techniques and the role of zero-knowledge proofs. In 2025 International Conference on Computing, Intelligence, and Application (CIACON) (pp. 1–7). IEEE. https://doi.org/10.1109/CIACON64654.2025.11189597

[9] Deng, Z., Han, D., Sun, J., & Sun, P. (2024). Applications and challenges of blockchain technology in data security and data governance. Academic Journal of Computing & Information Science, 7(6), 53–57. https://doi.org/10.25236/AJCIS.2024.070608

[10] Dhinesh, M., Priya, V., & Ramesh, S. (2024). Decentralized data management in IoT: Leveraging blockchain for improved integrity and trust. In 2024 International Conference on Advances in Computing, Communication and Materials (ICACCM) (pp. 1–6). IEEE. https://doi.org/10.1109/ICACCM61117.2024.11059040

[11] Farhan, M., Ali, S., & Khan, A. (2024). How decentralized systems reshaped data security. International Journal of Science and Research Archive, 12(01), 3191–3205. https://doi.org/10.30574/ijsra.2024.12.01.0989

[12] Gao, J., Saxena, A., & Chiu, B. H. (2024). Advancements in blockchain consensus mechanisms: Innovations, implications, and future prospects. International Journal of Computer Applications, 186(55), 1–13. https://doi.org/10.5120/ijca2024924262

[13] Ghadge, A., & Kara, S. (2024). Blockchain and smart contracts for sustainable and resilient supply chains. International Journal of Operations and Production Management, 44(2), 350–375. https://doi.org/10.1108/IJOPM-03-2023-0181

[14] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2024). Analyzing the role of blockchain in identity and access management. International Journal of Scientific Research and Analysis, 12(1), 1019–1035. https://doi.org/10.30574/ijsra.2024.12.1.1019

[15] Kumar, P., Sharma, R., & Verma, N. (2024). Blockchain and smart contracts for supply chain transparency and vendor management. World Journal of Advanced Research and Reviews, 23(02), 039–056. https://doi.org/10.30574/wjarr.2024.23.2.2262

[16] Luo, Y., Chen, X., & Zhang, H. (2024). Review of data security within energy blockchain: A comprehensive analysis of storage, management, and utilization. Energy and AI, 16, 100369. https://doi.org/10.1016/j.egyai.2024.100369

[17] Majdoub, A., & Atmani, B. (2025). Blockchain-based zero-knowledge proof protocol for privacy-preserving healthcare data sharing. Journal of Technology Informatics and Engineering, 4(1), 170–182. https://doi.org/10.56327/jtie.v4i1.296

[18] Morales-Díaz, A., Khanan, A., & Hakro, D. N. (2025). A blockchain-enabled smart contract architecture for enhancing transparency, traceability, and trust in global supply chain management. Computers, 15(3), 198. https://doi.org/10.3390/computers15030198

[19] R., S., Chirakarotu Nair, R., & Kumar Panakalapati, P. (2025). Promise of zero-knowledge proofs (ZKPs) for blockchain privacy and security: Opportunities, challenges, and future directions. Security and Privacy, 8(4), e461. https://doi.org/10.1002/spy2.461

[20] Saad, M., & Javed, A. (2024). Blockchain-based decentralized storage systems for sustainable data self-sovereignty: A comparative study. Sustainability, 16(17), 7671. https://doi.org/10.3390/su16177671

[21] Yang, X., Gülsena, G., & Özgür, K. (2025). Blockchain-enabled supply chain management: A review of security, traceability, and data integrity amid the evolving systemic demand. Applied Sciences, 15(9), 5168. https://doi.org/10.3390/app15095168

[22] Yusuf, A., & Aina, Y. A. (2024). Enhancing decentralized decision-making with big data and blockchain technology: A comprehensive review. Applied Sciences, 14(16), 7007. https://doi.org/10.3390/app14167007

[23] Zorlu, O., Kocak, C., & Ozturk, E. (2024). A blockchain-based secure framework for data management. IET Communications, 18(5), 301–315. https://doi.org/10.1049/cmu2.12781