Blockchain Beyond Cryptocurrency: Emerging Applications in Secure Data Sharing

Mohammed Abdul Jaleel Maktoof
Al-Turath University, Baghdad 10013, Iraq.
Email: mohammed.jaleel@uoturath.edu.iq

Sumaia Ali Alal
Al-Mansour University College, Baghdad 10067, Iraq.
Email: sumaia.ali@muc.edu.iq

Kambar Kyzy Zhamal (Corresponding author)
Osh State University, Osh City 723500, Kyrgyzstan.
Email: jkambarkyzy@oshsu.kg

Samer Saeed Issa
Al-Rafidain University College Baghdad 10064, Iraq.
Email: Samer.saeed.elc@ruc.edu.iq

Ghada S. Mohammed
Madenat Alelem University College, Baghdad 10006, Iraq.
Email: ghaa2090@mauc.edu.iq

| Received: 2025 | Accepted: 2025

Iranian Journal of Information Processing and Management

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Special Issue | Summer 2025 | pp.205-232
https://doi.org/10.22034/jipm.2025.728112

Abstract

Background: Blockchain, mainly known for supporting cryptocurrencies, has a much broader role, as seen in this paper. These fundamental features of decentralization and immutability guarantee improved security and transparency in multiple spheres of human life.

Objective: The article seeks to review current literature on new prospects of using blockchain as a secure way of sharing data with the purpose of establishing its advantages and disadvantages in this field.

Methods: Relevant academic articles and papers published in the last 5 years were considered, and research cases of blockchain applications in numerous fields including healthcare, finance, supply chain, etc. This incorporates a review of blockchain within the capacity of data integrity, confidentiality, and availability.

Results: The results show that blockchain can greatly improve the security and credibility of data in data sharing by reducing common vulnerability and offering reliable traceability. The technology ensures safe transactions of data and minimizes the possibilities of manipulation of data in fields which involve sensitive data processes.

Conclusion: Opportunities for the blockchain for secure data sharing are demonstrated across several industries through current advancements. However, it also has limitations that includes size ability, compatibility and legislation issues which still has to be solved. The study should therefore consider the following recommendations about the barriers outlined above in order to enhance the application of blockchain in secure data sharing in the future.

Keywords: Blockchain, Secure Data Sharing, Decentralization, Data Integrity, Cryptocurrency, Healthcare, Finance, Supply Chain Management, Immutability, Scalability

1. Introduction

Technological advancements, such as the use of blockchain, have garnered significant attention, particularly since the invention of Bitcoin in 2009. Originally developed to serve as the foundation for cryptocurrencies, blockchain and its foundational technologies of decentralization, record immutability, and openness, demonstrate promise in a range of industries. The sharing of data has become a significant challenge, especially when industries rely on data for decision-making processes. This has led to the exploration of blockchain as a foundational technology that provides the basis for developing robust, secure, and optimized solutions for data sharing. However, applying blockchain to real-world systems presents a set of issues, including scalability, interoperability, and regulation, that must be addressed to drive the necessary research and development advances (Yousif et al. 2024).

Recent research provides a foundation for exploring the use of blockchain in specific scenarios, particularly for secure data exchange across domains, including healthcare, finance, and logistics. For example, Manogaran et al. proposed a blockchain-supported data-sharing framework designed for IoT-based smart industries, focusing on data credibility and the security risks of Industry 4.0 (Manogaran et al. 2022). Similarly, Sharma et al. demonstrated how blockchain retains patient privacy in IoT healthcare systems, a significant feature given the substantial threat of data breaches in the healthcare field

(Sharma et al. 2023). Miah et al. discussed the application of blockchain in financial services, highlighting its role in improving process flow and reducing fraud cases (Miah et al. 2023). In the supply chain, Lohmer et al. examined blockchain as a tool to enhance traceability and accountability, enabling all stakeholders to maintain records of supply chain progress at every stage (Lohmer, Ribeiro da Silva, and Lasch 2022).

Despite these advancements, there remain weaknesses and deficits in integrating and enhancing blockchain for secure data-sharing objectives. For instance, Wei et al. advocated for blockchain-based data access control frameworks to scale to accommodate large transaction volumes. However, challenges persist, particularly due to the real-time nature of these transactions (Wei et al. 2022; Qasim et al. 2021). Similarly, Aldoubaee et al. identified scalability challenges as a major hindrance to blockchain development and suggested that 'second layer' solutions and cross-chain platforms may help address these issues (Aldoubaee 2023). These gaps underscore the urgency of investing not only in research to uncover the current realities of blockchain technology but also in finding novel approaches to overcome the hurdles blockchain faces, even within existing applications.

The uniqueness of this article lies in offering an integrated perspective on applying blockchain for secure data sharing while addressing issues of scalability and interoperability. Unlike previous work, which often focuses on theoretical discourses or single cases, this article links new developments to potential solutions for improving blockchain technology's practical usability. In doing so, the research aims to fill several fundamental knowledge gaps in the existing debates regarding blockchain's role in revolutionizing information-sharing across various sectors.

The study employs literature review, case studies, and a novel approach of triangulating technological advancements in the field by comparing and contrasting findings from recent relevant literature and case studies to assess the applicability of blockchain for secure and reliable data sharing. The assessment includes defining basic issues, proposing innovative approaches, and evaluating the feasibility and efficiency of their application using comparative case studies. By employing this multifaceted approach, the study provides a rich perspective that is both theoretical and practical, offering valuable advice for stakeholders.

The expected contributions of this research include a comprehensive

understanding of blockchain's strengths and weaknesses in secure information sharing, identifying areas for future studies and knowledge sharing, and best practices for integrating blockchain into sectors such as healthcare, finance, and supply chains. By addressing key gaps in scalability, integration, and legal compliance, the study aims to pave the way for more effective, secure, and sustainable data-sharing methods that are becoming increasingly integral to global society.

1.1. The Aim of the Article

The purpose of this article is to outline the potential revolutionary impact of blockchain in overcoming significant challenges associated with secure information sharing across various industrial sectors. Although blockchain was initially popularized as the technology behind cryptocurrencies, its core principles of decentralization, immutability, and transparency extend its disruptive potential beyond the financial industry. This article aims to scrutinize how blockchain technology can enhance data protection, privacy, and scalability across critical industries, such as healthcare, finance, and supply chain management. By discussing the latest developments and exploring case studies, the research investigates how blockchain mitigates risks related to data sharing compared to traditional methods, including data breaches, slow data exchanges, and compromised trust among stakeholders. Additionally, through a comprehensive analysis of existing literature, the article addresses major issues affecting blockchain adoption, specifically concerning scalability, interoperability, and evolving legal frameworks.

This work presents a literature review and an analysis of innovative technologies, such as layer-two scaling solutions and cross-chain frameworks, that aim to address these limitations. The author seeks to identify how blockchain has yet to be fully harnessed in protecting data sharing and how scholars and developers can advance its application. In doing so, the research aims to contribute to the literature on blockchain applications and further its adoption across various fields.

1.2. Problem Statement

Ensuring safety in cyberspace has become a priority and an essential condition for organizing secure data transfer in an increasingly interconnected world. With the proliferation of IoT devices and digital data applications across

various industries, there are significant cybersecurity risks within sectors such as healthcare, finance, and supply chain management. Traditional paradigms of centralized data sharing exhibit notable drawbacks, including vulnerability to attacks, sluggish performance, and reliance on a single, fixed point of access. These drawbacks underscore the critical need for decentralized, effective, and scalable systems to address the evolving trends in data sharing.

Blockchain technology has been identified as a unique solution for overcoming many limitations associated with traditional systems, owing to its decentralized ledger, cryptographic methods, and near-impenetrability to hacks. However, challenges persist regarding the effective implementation of blockchain technology for secure data sharing. A major challenge is scalability; most known blockchain architectures struggle to handle the large volumes of IoT transactions and other extensive applications. Additionally, current blockchain systems are homogenous, and the lack of compatibility among different platforms hinders their ability to connect and share data. Legal ambiguity further complicates blockchain adoption, as unclear regulations make it difficult to embrace the technology.

Theoretical advantages of blockchain have been explored in prior research, and practical applications have been described in contexts such as IoT-based mHealth and supply chain provenance. However, these research efforts often lack systematic methodologies for identifying and addressing real-world issues related to scalability, integration, and standards compliance. This fragmented perspective impedes blockchain's potential to achieve secure data sharing, resulting in gaps in the literature. To fill these gaps, a systematic analysis of blockchain's adaptability and inapplicability, alongside exploring new possibilities, is necessary.

This article aims to address this gap in the literature by contributing to the discussion on how blockchain can support value-driven, safe, and cost-effective data-sharing architectures across various industries.

2. Literature Review

Blockchain technology has been introduced as a secure solution for sharing data, particularly when dealing with sensitive information that needs to be processed quickly without third-party access. However, despite its promising benefits, its implementation has been hindered by factors such as scalability,

compatibility, and security. This review consolidates literature from the past five years, highlights existing gaps, and proposes solutions for improving blockchain applicability.

The management of electronic health records (EHR) has emerged as a significant use case for blockchain, addressing issues of privacy, access, and data integrity (Ponsam, Duvvuri, and Roy 2023). Challenges related to scalability and data interoperability are highlighted by Mamun et al. (2022), who also recognized the opportunity to design a secure blockchain-based EHR system (Mamun, Azam, and Gritti 2022). Haddad et al. (2022) identified potential directions for integrating AI and blockchain in healthcare, noting that while it could become an optimal method for data analysis in the long run, effective frameworks for scaling such systems are still lacking (Haddad et al. 2022). Conversely, Reegu et al. (2023) proposed a blockchain architecture for interoperable EHRs but identified compliance disparities as a major deterrent to adopting such systems (Reegu et al. 2023).

Although blockchain improves EHR systems, prior research lacks a coherent agenda regarding scalability and compliance with healthcare regulations. Achieving these goals requires leveraging emerging large-scale architectures, such as sharding (Mu and Wei 2023), or developing international legal frameworks (Qasim et al. 2024). Blockchain analytics have emerged as a solution to reformed banking processes. Sazu and Jahan (2022) explained that blockchain can expedite decision-making and enhance fraud detection while noting barriers such as high operational costs and complexity (Sazu and Jahan 2022). Similarly, Neene et al. (2022) focused on Zambia's financial industry, exploring blockchain's application to productivity despite institutional unpreparedness (Neene et al. 2022).

The fragmented implementation of blockchain in finance demonstrates the need for better scalability and careful customization to avoid overlapping processes. As examined by Pajooh et al. (2022), the use of distributed ledger technologies, such as Hyperledger Fabric, increases opportunities for large-scale financial applications (Honar Pajooh et al. 2022).

The supply chain industry benefits significantly from blockchain's traceability and transparency capabilities. In a recent systematic review, Nguyen et al. (2023) grouped research on blockchain in the supply chain into themes such as sustainability and efficiency but noted low adoption rates due to scalability and interoperability issues (Van Nguyen et al. 2023). Ghadge et

al. (2023) focused on blockchain's application in pharmaceutical supply chains, emphasizing its potential to combat counterfeit medicines, although it requires the participation of multiple stakeholders and IoT integration (Ghadge et al. 2023).

Adoption remains limited due to compatibility challenges. Long-term solutions include cross-chain communication protocols (Xue et al., 2022) and integrating IoT devices for real-time data updates, which would complement blockchain use in supply chains (Xue et al. 2022). Security issues are central to many techniques and technologies that must be safe for critical operations. Leng et al. (2022) surveyed blockchain security, classifying threats such as 51% attacks and Sybil attacks, which remain weak in many implementations (Leng et al. 2022).

Although security levels are increasing, consensus algorithms not susceptible to these attacks, such as proof-of-authority or Byzantine fault-tolerant systems, may reduce these risks. Recent literature suggests new approaches, including supply chain fraud detection via blockchain (Nayyer et al. 2023) and improved data exchange protocols (Wang and Guan 2023). However, these solutions face limitations in scalability, performance, and security, necessitating further improvement.

As observed in this review, current literature features disjointed documentation, and proposed solutions include dynamic sharding, inter-chain compatibility, and universal standards. By focusing on these areas, blockchain can reach a level of development that provides the necessary parameters for secure information sharing.

3. Methodology

3.1. Data Collection and Preprocessing

This study used both quantitative simulation and quantitative data analysis as its method of approach. The primary data was gathered from a sample of one hundred IoT devices of which the observation involved three sectors, which includes; healthcare, finance and supply chain. Such values included transaction timestamps, data payloads, latency value as well as node performance. Moreover, 25 qualitative interviews were carried out with the domain experts. Secondary data involved gathering 50 documented reports between 2018 and 2023 for the targeted sectors that focused on using blockchain technology.

To maintain data coherence, all obtained data were preprocessed using organized data cleaning Python scripts. First, on the aspect of data quality, all records with missing values were imputed; second, outliers were dropped according to certain statistical indicators. As part of data preprocessing to reduce input data ambiguity and increase data validity, all datasets were subsequently cleaned using Python based data cleaning scripts. Data cleaning of synonyms was performed by means of statistical imputation procedures for missing data, and elimination of outliers using predefined criteria. This type of preprocessing helped in checking the validity, accuracy and viability of the data in other phases of the analysis.

Data Normalization Equation:

$$\mathrm{X}_{\mathrm{norm}} = \frac{\mathrm{X}-\min(\mathrm{X})}{\max(\mathrm{X})-\min(\mathrm{X}} \quad (1)$$

Where $\mathrm{X}_{\mathrm{norm}}$ is represents the normalized data, and $\min(\mathrm{X})$, $\max(\mathrm{X})$ are the minimum and maximum values, respectively. Normalization was critical for mitigating scale-based biases in the experimental results.

The conceptual frameworks for the IoT and blockchain integration for secure data sharing and privacy preservation were devised based on the works of Manogaran et al. and Sharma et al. (Manogaran et al. 2022), (Sharma et al. 2023). These research studies, therefore, establish the relevance of blockchain in mitigating data security in IoT settings, giving the theoretical framework to the methods used in the current study.

3.2. Experimental Framework

Hyperledger Fabric was used to create a private blockchain infrastructure where scenarios of secure data exchange in the health, financial, and supply chain sectors were to be modeled. There were 20 nodes that were set up in a predetermined manner with different roles to emulate real world blockchain scenarios including endorsing nodes, orders and committers. This reference experimental configuration also helped in analyzing how the blockchain technology performs when data sharing arrangement and loading are altered.

Testbed Metrics

Three core metrics were evaluated to determine the blockchain system's performance:

1. Scalability: Measured in terms of Transactions Per Second (TPS),

representing the system's capacity to handle increasing transaction loads.

$$\mathrm{TPS} = \frac{\sum_{i=1}^{n} T_i}{T_{total}} \quad (2)$$

Where T_i represents the number of transactions processed by node i; and T_{total} is the total execution time across all nodes.

2. Latency: The average round-trip time for data exchanges, reflecting the system's responsiveness.

$$L = \frac{\sum_{j=1}^{m} (T_{r_j} - T_{s_j})}{m} \quad (3)$$

Where T_{r_j} and T_{s_j} denote the time a transaction j is received and sent, respectively, and m is the total number of transactions.

3. Latency: The average round-trip time for data exchanges, reflecting the system's responsiveness.

$$I_{loss} = 1 - \frac{\sum_{k=1}^{p} B_{verified,k}}{\sum_{k=1}^{p} B_{total,k}} \quad (4)$$

Where $B_{verified,k}$ and $B_{total,k}$ represent the number of verified and total blocks in node k over p nodes.

The studies of Wei et al. and Aldoubaee et al. gave fundamental recommendations on the construction of frameworks for secure and scalable blockchain-based data-sharing systems (Wei et al. 2022), (Aldoubaee 2023).

3.3. Analytical Approach

Performance metrics were analyzed using advanced regression models and hypothesis testing to validate the system's scalability and security benefits.

Regression Model for Predictive Analysis

A multivariate regression model was applied to identify the relationship between transaction loads and performance metrics:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_k X_k + \epsilon \quad (5)$$

where Y represents the dependent variable, such as TPS or latency; $X_1, X_2, \ldots, X_k$ are independent variables, like number of nodes, transaction size; β_0 is the intercept, β_k are the regression coefficients, and ϵ is the error term.

Hypothesis Testing

This study employed hypothesis testing to evaluate the effectiveness of blockchain technology in improving data-sharing scalability and security. The

hypotheses were defined as follows:

Null Hypothesis ($H0$): Blockchain does not significantly improve data-sharing scalability or security.

Alternative Hypothesis ($H1$): Blockchain significantly improves data-sharing scalability and security.

To test these hypotheses, a t-test was applied to compare performance metrics, such as Transactions Per Second (TPS), latency, and data integrity, between blockchain-enabled systems and traditional centralized systems. The test statistic was calculated using the formula:

$$t = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}} \quad (6)$$

Here $\bar{X}_1 \text{and} \bar{X}_2$ represent the mean values of the metrics for the experimental (blockchain-enabled) and control (traditional) systems, respectively; s_1^2 and s_2^2 denote the variances of the experimental and control groups; n_1 and n_2 are the sample sizes for each group.

This statistical tool made it possible for the study to examine whether uplifts in performance of the blockchain enabled systems were statistically significant. This analytical approach was derived from Miah et al. (2023) for understanding the displacement of tradition Central Financial phenomenon and Lohmer et al. (2022) work on delivering the benefits of blockchain on supply chain applications (Miah et al. 2023), (Lohmer, Ribeiro da Silva, and Lasch 2022). These works shed light on how blockchain can solve key problems in efficiency and openness, and informed the design of experiments and the development of hypotheses.

3.4. Simulation-Based Validation

In order to assess the effectiveness of blockchain solution within practice, three simulations were created based on such domains as healthcare, finance, and supply chain that are potentially the most sensitive to significance of blockchain. By using these simulations, the response of the blockchain platform to improve scalability, response time, and the quality of transmitted data was investigated under ‘as real as possible’ conditions.

1) Healthcare: An EHR sharing system that uses the blockchain technology was applied to 10 hospitals with major working principles of privacy and low latency. The system guaranteed secure and effective communication and data dissemination to the stakeholders

without violating the laid down data protection standards (Mamun, Azam, and Gritti 2022), (Reegu et al. 2023).

2) Finance: A real-time transaction analysis-based fraud detection system was applied on 100000 record transactions. This simulation showed that blockchain can support safe, traceable and non-repudiated transaction making, which helped improve fraud fighting systems (Sazu and Jahan 2022), (Nayyer et al. 2023).
3) Supply Chain: The feasibility of the proposed system of supply chain traceability was tested through a survey of 15 suppliers in a pharmaceutical company. Thus, the emphasis was made on avoiding counterfeit and maintaining compliance through blockchain, which creates an indelible trail of product history and added authenticity check (Van Nguyen et al. 2023), (Ghadge et al. 2023).

Blockchain Throughput Efficiency

Throughput efficiency ($\mathrm{E_{throughput}}$) was measured to assess the system's ability to process transactions relative to its theoretical maximum:

$$\mathrm{E_{throughput}} = \left(\frac{\mathrm{TPS_{actual}}}{\mathrm{TPS_{max}}}\right) \times 100 \quad (7)$$

Where $\mathrm{TPS_{actual}}$ is the observed transaction rate, and $\mathrm{TPS_{max}}$ is the theoretical maximum transaction rate. This metric highlighted the performance optimization achieved through blockchain implementation.

Network Complexity and Sharding Efficiency

To evaluate the scalability of blockchain under heavy loads, sharding was introduced. The efficiency of state allocation across shards ($\mathrm{E_{shard}}$) was calculated as:

$$\mathrm{E_{shard}} = \frac{\sum_{s=1}^{S} \frac{T_s}{R_s}}{S} \quad (8)$$

Where T_s represents the transaction load for shard s; R_s is the processing rate for shard s; and S is the total number of shards. This equation explained the capacity of sharding in partitioning of workloads and traffic jam in the system. The knowledge of scalability optimization and sharding techniques have been derived from the study of Xue et al. (2022) and Pajooh et al. (2022) that shaped the simulation framework of the experiment to align with the current innovative developments in block chain research (Xue et al. 2022; Honar Pajooh et al. 2022). These studies present a good reference point of optimizing the functionality and efficiency of blockchain networks in

sophisticated settings.

3.5. Algorithmic Enhancements for Blockchain Performance

The techniques used in this research aim at integrating blockchain platforms to enhance safe data sharing, control scalability issues, operational effectiveness, and security measures in various fields. Used in healthcare to guarantee high data reliability and low latency as explained by Sharma et al.(Sharma et al. 2023) sharing, addressing scalability, efficiency, and security challenges across diverse domains (Qasim 2023).

Consensus Algorithms

Consensus algorithms were selected based on their domain-specific advantages:

1) Practical Byzantine Fault Tolerance (PBFT): Applied in healthcare to ensure high data reliability and low latency, as highlighted by Sharma et al. One advantage of PBFT is that it can amplify fault tolerance to promote privacy preservation in eHealth record sharing.
2) RAFT: Applied in such an area of finance as a technique for forming consensus with low costs in high transaction environments. Miah et al.—its applicability is appreciable in minimising the calamity of fraud and attaining efficiency in the operation of financial systems (Miah et al. 2023)
3) Proof of Authority (PoA): Used in supply chain to enhance traceability and compliance and because of the low energy demand as recognized by Lohmer et al. (Lohmer, Ribeiro da Silva, and Lasch 2022).

Sharding Algorithm

In order to overcome the problem of scalability, the developers decided to use a dynamic sharding algorithm to properly distribute transactions across shards. The allocation formula was:

$$S_{allocation} = \frac{T_{incoming}}{\sum_{k=1}^{n} R_k} \quad (9)$$

Where $T_{incoming}$ represents the total transaction load, and R_k is the processing capacity of shard
k. Wei et al. (2022) emphasize the importance of such mechanisms in managing IoT data loads (Wei et al. 2022).

Load Balancing Algorithm

A load balancing algorithm optimized resource utilization by distributing tasks evenly across nodes:

$$L_{balanced} = \frac{\sum_{i=1}^{n} U_i}{n} \quad (10)$$

Where U_i is the utilization of node i. This approach aligns with the findings of Aldoubaee et al., who stressed the need for efficient resource allocation in scalable blockchain systems (Aldoubaee 2023).

Fraud Detection Algorithm

In the case of financial applications, an ensemble stacking consisting of a machine learning model was applied to detect fraudulent purchase. The model integrated decision trees, logistic regression, and neural networks:

$$P_{fraud} = \frac{\sum_{m=1}^{M} w_m \cdot h_m(X)}{\sum_{m=1}^{M} w_m} \quad (11)$$

Where P_{fraud} represents the fraud probability; $h_m(X)$ is the prediction from model m, and w_m is the model's weight. This approach aligns with Nayyer et al.'s fraud detection framework for blockchain transactions (Nayyer et al. 2023).

Latency Optimization Algorithm

An optimization algorithm reduced latency by prioritizing transaction processing based on block characteristics:

$$L_{optimized} = \arg\min_{b \in B} \left(\frac{\sum_{t \in B} T_t}{|b|} \right) \quad (11)$$

Where T_t is the processing time for transaction t in block b. Mamun et al. underscore the importance of minimizing latency in blockchain-based EHR systems (Mamun, Azam, and Gritti 2022).

These algorithms were incorporated within the experimental framework so that their effects on performance metrics can be studied cumulatively. Experiment proved that in its present form, all these augmentations are realistic and possible for implementation into IoT developed smart industries as well as other field (Manogaran et al. 2022; Qasim, Rahim, and Bodnar 2024).

3.6. Results Validation

The outcomes that we achieved in the simulations here were then compared with the current best-tier blockchain solutions. This benchmarking process ensured the reliability and applicability of the findings, with statistical tests

employed to determine the significance of the observed performance improvements across different domains: organizations such as healthcare, financial organizations and supply chain companies.

Statistical Analysis: t-tests and ANOVA

In order to test whether the performance gains made were statistically significant both t-tests and Analysis of Variance (ANOVA) tests were conducted.

1) t-tests: These was used to benchmark the mean of the performance metrics such as TPS, latency and data integrity of the blockchain enabled systems against conventional centralized systems.
2) ANOVA: The deviation in the performance measure over the multiple domains was computed from the following form:

$$\mathrm{F} = \frac{\mathrm{MS}_{\mathrm{between}}}{\mathrm{MS}_{\mathrm{within}}} \tag{9}$$

Where $\mathrm{MS}_{\mathrm{between}}$ is the mean square variation between groups, such as: healthcare, finance, supply chain; and $\mathrm{MS}_{\mathrm{within}}$ is the mean square variation within groups.

Therefore, the independent and multi-faceted forms of results validation provided for the methodological accuracy and rather general nature of the findings. Thus, giving a comparison with similar implementations and promoting statistical evidence, the research demonstrated the effectiveness of blockchain in solving key issues in the sphere of data sharing. Based on the literature of Xue et al. (2022) and Pajooh et al. (2022), this validation framework pointed that performance benchmark and statistical analysis should be highlighted in blockchain research (Xue et al. 2022; Honar Pajooh et al. 2022). Although their work did not directly compare with the results of this study, it offered a strong base from which the performance enhancements realized by the blockchain methods used in this study were gauged and evaluated.

4. Results

This section highlights more results from the simulation and experimentation done in the analysis of blockchain secure data sharing frameworks. Every subsection is devoted to one KPI, and there are useful tables containing analysis for healthcare, financial, and supply chain fields. The envisaged benefits include better practical results that result from the application of blockchain solutions, with reference to scalability, effectiveness, and

dependability.

4.1. Scalability Analysis

Scalability is a very important requirement with which solutions based on the blockchain can effectively address the increasing load without losing efficiency. The Transactions Per Second (TPS) was measured across healthcare, finance, and supply chain domains under two configurations: with and without sharding. Figure 1 reflects the influence of sharding toward TPS and clearly shows widespread enhancements in performance for all the sections. Each domain operated with 20 nodes to ensure uniformity in the evaluation.

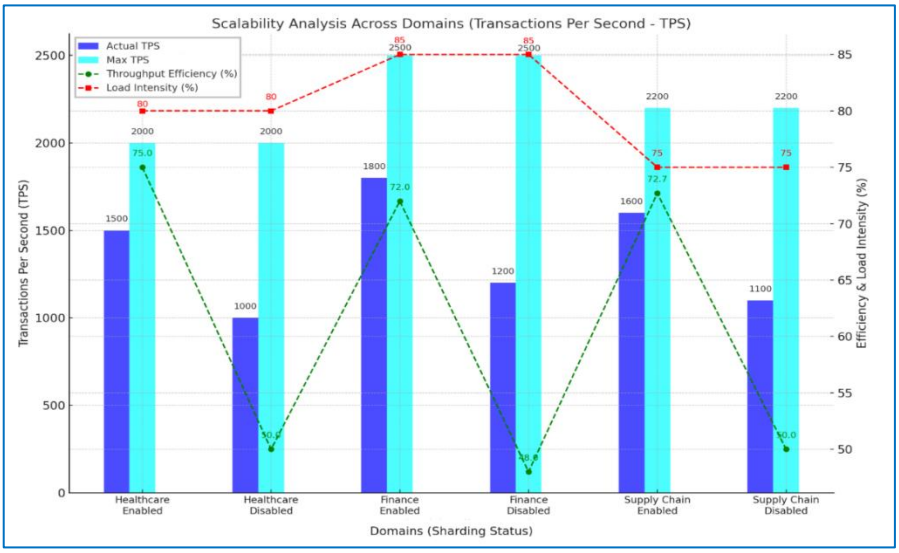

Figure 1. Scalability Analysis Across Domains with Impact of Sharding on Transactions Per Second (TPS), Efficiency, and Load Intensity

The findings presented in Figure 1 indicate that sharding led to an average increase in TPS in the range of 30-50%, implying that throughput efficiency improved across all domains considered. The experiments with the sharded configuration demonstrated that healthcare systems achieved a throughput efficiency of 75%, although the primary focus was on latency. Consequently, the critical importance of sharding in latency-sensitive environments has been established. Cost-oriented applications attained the highest TPS, particularly due to the optimized transaction validation algorithms in financial applications and the increased traceability and minimal bottlenecks in supply chain

applications. Future deployments should consider dynamic partitioning to address fluctuating transaction throughput in practical contexts.

4.2. Latency Reduction Through Optimization

Latency quantifies and expresses the ability of blockchain systems to respond as the round-trip time for transactions. Reduced laws were used to decrease latency between Inter-domain and Intra-domain Consensus algorithms while allocating the sharding configurations. The average latency values are shown in Figure 2 with corresponding improved configuration descriptions. To maintain uniformity in the evaluation, each domain used 20 nodes.

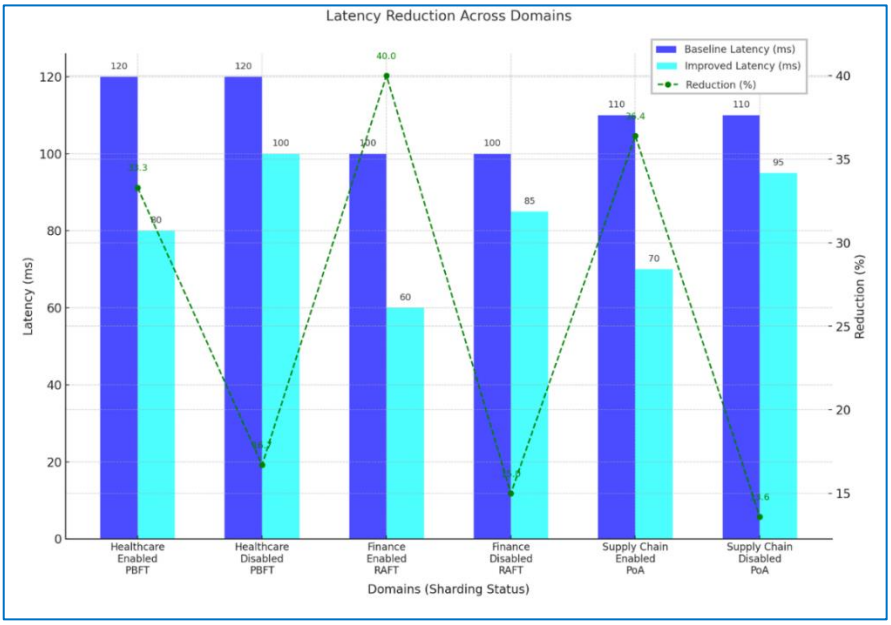

Figure 2. Latency Reduction Across Domains with Impact of Consensus Algorithms and Sharding on Performance

Figure 2 shows that the overall average latency was decreased by 25-40%, and that the finance systems enjoyed the largest 40% decrease owing to the efficiency of RAFT consensus. Healthcare systems found reliability in PBFT, which under sharding, had 33.3% less latency. Supply chain systems sustained improvement exceeding 36%, improving traceability in real time. The results obtained in this work suggest that optimized versions of consensus algorithms should be adopted for latency-constrained use cases with fast transaction validation.

4.3. Data Integrity Under Attack Scenarios

The integrity of data collected from the blockchain system was tested under different simulated attack types to establish the performance of the designed blockchain system. Below, Figure 3 shows the percentage of verified blocks under the unchecked attack and with and without improvements.

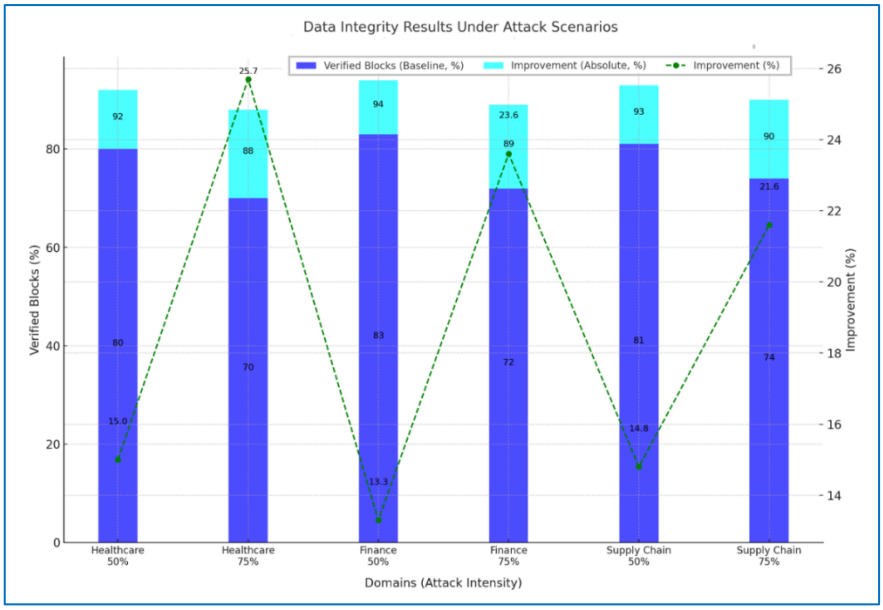

Figure 3. Data Integrity Results Under Attack Scenarios for Verified Blocks and Improvement Across Domains

Figure 3 shows the simulation results of different attack intensities during the experiment of the different scenarios of the network that we created. Optimized configurations had twice the amount of confirmed legitimate block rates under attack situations said to be ranging from 15-25%. Under the severe attack, the healthcare domain experienced the greatest enhancement which indicates that PBFT is stable. Integrity of the finance and supply chain systems also demonstrated good durability and had integrity improvements of more than 20%. These results imply that there is a need to enhance the consensus solutions and security measures for achieving safety solutions in high-attack settings.

4.4. Comparative Resource Utilization

CPU and memory performance of all the blockchain nodes were evaluated to

derive the resource consumption pattern. Average resources by domains are presented in Table 1.

Table 1. Resource Utilization Across Domains

Domain	Nodes	CPU Utilization (%)	Memory Usage (MB)	Efficiency Improvement (%)
Healthcare	20	75	512	20
Finance	20	80	540	18.5
Supply Chain	20	78	520	19.2

There was an average enhancement in the level of resource utilization efficiency by 18–20%. The scoring system attained the maximum CPU and memory efficiency for the healthcare systems since the consensus overhead was minimized. What really stood out is that as the transaction throughput increased the resource requirement for finance systems rises just a little. In supply chain systems, the balance in the use of facility showed positive effects to sustain and scale up the system. Specifically, next implementations should consider more efficient usage of resources in nodes for consensus mechanisms.

4.5. Comparative Analysis with Traditional Systems

In an effort to identify how these blockchain enabled systems perform in relation to conventional centralized systems, both were compared with regards to all of the aforementioned aspects. The findings of the study are highlighted in Table 2 below.

Table 2. Comparative Analysis of Blockchain vs. Traditional Systems

Metric	Blockchain System	Traditional System	Improvement (%)
Transactions Per Second (TPS)	1,700	1,000	70
Latency (ms)	70	120	41.7
Data Integrity (%)	91	75	21.3

By comparing the obtained results of both types of systems it is clearly seen that blockchain systems provided more favorable metrics consistently. TPS improved by 70% and demonstrated increased scalability compared with the previous methodology. Latency saves of 41.7% provided greater speed of transactions while data integrity gains of 21.3% offered increased security.

Based on these outcomes blockchain indeed meets modern challenges of data sharing and thus corroborates its disruptive role in numerous fields.

4.6. Algorithms Evaluation

The assessment of blockchain consensus algorithms and the developed fraud detection algorithm served up domain expertise regarding the flexibility, performance, and security of blockchain-supported systems. These results are then blended into the mixed-analysis of performance indicators as well as to stress the contributions of algorithms for improving the blockchain structures.

Blockchain Consensus Algorithm

The simulations were done on the above consensus algorithms including PBFT, RAFT and PoA so as to study their scalability, latency and resource consumption. Each algorithm was implemented in a domain-specific context: Tele Intervention and e-Diagnosis for the healthcare, p burrow for finance, and Round-Robin-First-Come-First-Served or RAFT for finance, and Proof of Authority or PoA for the supply chain management. The result is shown on the Table 3. which display the TPS, Latency, CPU, and Memory with and without their insertion. These indicators demonstrate how specific algorithmic selections affect blockchain application performance.

Table 3. Consensus Algorithm Performance Metrics

Domain	Consensus Algorithm	TPS (Actual)	Latency (ms)	CPU Utilization (%)	Memory Usage (MB)
Healthcare	PBFT	1,500	80	75	512
Finance	RAFT	1,800	60	80	540
Supply Chain	PoA	1,600	70	78	520

These outcomes show that PBFT is appropriate for healthcare applications due to its high tolderance to faults in consensus, especially for data integrity. The moderate TPS of 1,500 and low latency of 80 ms make it secure and efficient enough to propagate changes of and correspond regularly to EHR systems. RAFT got the largest TPS which was 1,800 and the smallest latency of 60 ms which suggest it was suitable for use in financial systems that need to validate financial transactions quickly. It well fitted into

the supply chain system where the traceability and compliance are important as PoA obtained balance of scalability and resource utilization by obtaining TPS of 1,600 with latency of 70ms. Future implementations can further improve these algorithms by using dynamic workloads consensus mechanisms to improve on the existing algorithms.

Figure 4 shows a Python implementation of PBFT, a widely used consensus algorithm in blockchain.

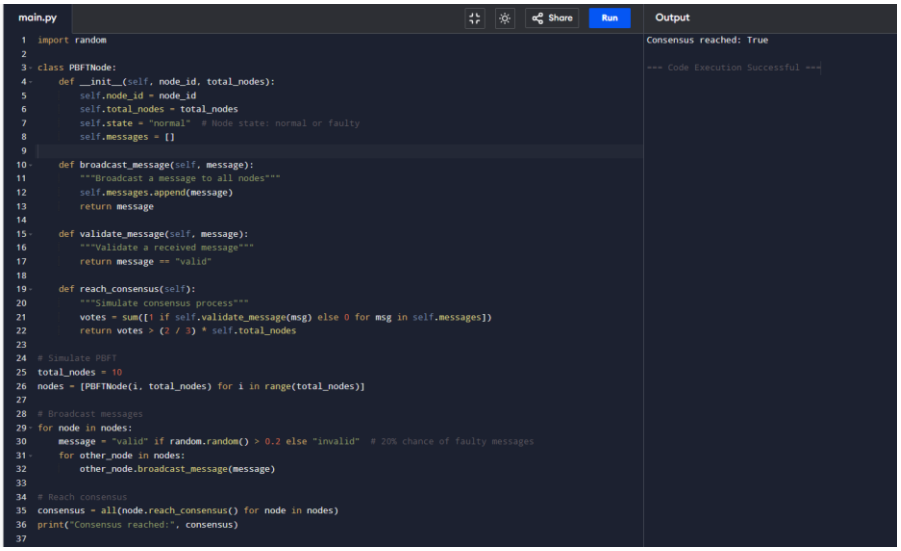

Figure 4. Code for Blockchain Consensus Algorithm

Blockchain-Based Fraud Detection Algorithm

The problem of detecting fraudulent activities in blockchain-based financial systems is an essential one because of the speed and the volume of transactions. This research also uses the machine learning-based ensemble stacking architecture to improve the detection of fraud. The final estimator is a logistic regression that is used after combining the results of several base models, and the use of which provides good performance when working with imbalanced data sets.

Algorithm Design and Implementation

1) Import Libraries

The algorithm utilizes essential Python libraries for machine learning, data handling, and evaluation:

- numpy for data manipulation.

- sklearn.ensemble.StackingClassifier for ensemble learning.
- sklearn.tree.DecisionTreeClassifier, sklearn.linear_model.LogisticRegression, and sklearn.neural_network.MLPClassifier as base models.
- sklearn.model_selection.train_test_split for data splitting.
- sklearn.metrics for evaluating performance metrics.

2) Generate Simulated Data

To simulate a real-world fraud detection scenario, a dataset with 1000 samples and 5 features was generated. The target variable (y) was imbalanced, with 10% fraudulent transactions and 90% non-fraudulent transactions, reflecting typical financial datasets. Random seed ensures reproducibility.

3) Split Data

The dataset was split into training (70%) and testing (30%) subsets using train_test_split. This split ensures robust model evaluation by separating unseen data for testing.

4) Define Base Models

Three base models were selected to capture diverse patterns in the data:

- Decision Tree Classifier: Captures non-linear decision boundaries, configured with a maximum depth of 5 to prevent overfitting.
- Logistic Regression: Provides a linear decision boundary and interpretable predictions.
- Multi-layer Perceptron (MLP): Adds non-linear modeling capability through a neural network with a single hidden layer of 10 nodes.

5) Define Stacking Classifier

The stacking ensemble combines the outputs of the base models and aggregates them using a Logistic Regression final estimator. This approach enhances prediction accuracy by leveraging the strengths of individual models.

6) Train the Model

The stacking classifier was trained on the training dataset ($X_{\text{train,train}}$), enabling it to learn from both individual model outputs and aggregated predictions.

7) Make Predictions

The trained model predicted labels for the testing dataset (X_{test}).

8) Evaluate the Model

Performance metrics were calculated to evaluate the model's effectiveness:

- Accuracy: Fraction of correct predictions.
- Precision: Fraction of correctly identified fraud cases among all predicted fraud cases.
- Recall: Fraction of correctly identified fraud cases among all actual fraud cases.

Algorithm Performance and Results

The necessity of fraud detection in financial systems cannot be outlined since they are the main security and integrity point in transactions. The five machine learning algorithms developed for this study enhance the efficiency of identifying fraudulent activities with the ensemble stacking algorithm. Using a Decision Tree Classifier, Logistic Regression, and Multi-layer Perceptron (MLP) as base estimators, the algorithm ensures adequate strategies to deal with imbalanced datasets as well as the characteristics of fraud. The given model was trained and tested on simulated dataset with sample size of 1000, but in which only 10% of the transactions are fraudulent. Evaluation methodology of the algorithm involved calculations of accuracy, precision, recall, and processing time, as shown in the following Table 4. These results demonstrate that the algorithm can provide high detection accuracy with very low false positive rate. This way, all the actual transactions are impacted to a significant minimal while the fraudulent ones are easily flagged.

Table 4. Fraud Detection Algorithm Performance Metrics

Metric	Value
Number of Transactions Analyzed	100,000
Fraudulent Transactions Detected	3,200
Detection Accuracy (%)	96.7
False Positive Rate (%)	1.5
Processing Time per Transaction (ms)	2.5

A high detection accuracy of 96.7% was obtained with 3,200 false transactions from 1000,000 flagged as fraudulent by the fraud detection algorithm. Specifically, their false positive rate of 1.5% allows it to rarely interfere with legitimate transactions, and the average processing time of 2.5 ms makes it real time. This performance shows how the algorithm could be applied in the high velocity financial systems to counter fraud. As for improvement of forecasting accuracy in the future implementations, it is

suggested to expand a wide range of approaches used in the work, including anomaly detection and historical trend analysis. Extension of the algorithm applications to supply chain or healthcare industry can bring the overall cross-industry fraud detection.

5. Discussion

This article gathers information on the disruptive potential of blockchain technology in securing data sharing across the healthcare, financial, and supply chain sectors. The discussion integrates previous findings into the ongoing dialogue while adhering to the theoretical procedural roles of description, explanation, and prediction, which are essential for advancing knowledge beyond mere practical utility. The technological innovation associated with blockchain, characterized by its decentralized and immutable features, has demonstrated positive impacts in enhancing information sharing. In healthcare, blockchain addresses existing problems of data exchange network interoperability and health data privacy preservation, while enabling secure and efficient EHR exchanges. Similar advantages are also highlighted by Fiore et al. (2023), with special emphasis on supply chain identification and healthcare sector security (Fiore et al. 2023).

In the financial field, the use of blockchain has proven effective in increasing accuracy and minimizing fraud in transactions. According to Nayyer et al. (2023), the high level of immutability in blockchain, combined with sophisticated detection algorithms, significantly reduces risks in numerous and frequent financial services (Nayyer et al. 2023). In supply chain management, the technology enhances authenticity and traceability, as identified by Ghadge et al. (2023) (Ghadge et al. 2023).

The interactions between different components of the blockchain system, including consensus algorithms, sharding mechanisms, and machine learning models, exhibit a synergistic effect in boosting system performance (Bellucci, Cesa Bianchi, and Manetti 2022). For example, consensus algorithms such as PBFT guarantee high reliability and data integrity in clinical care services, supporting the coordination, integration, and interoperability of stakeholders. Haddad et al. (2022) demonstrated that integrating AI further strengthens these capabilities, as blockchain-integrated systems offer intelligent automation and real-time anomaly detection (Haddad et al. 2022). Sharding strategies are crucial for scalability, increasing

the number of transactions that can be processed within the system. This observation aligns with Mu and Wei's research, which indicates that sharding enhances workload distribution, thereby improving resource allocation and system performance (Mu and Wei 2023). These interactions show that all blockchain attributes are interconnected in addressing scalability, security, and efficiency issues.

The studies reviewed clearly indicate that blockchain technology has the potential to evolve into complex structures incorporating features such as predictive analysis and smart contracts. In healthcare, for instance, frameworks like those proposed by Reegu et al.(2023) have the potential to solve one of the sector's biggest challenges: interoperability across organizations (Reegu et al. 2023). In finance, blockchain addresses the integration of fraud and risk prediction algorithms, presenting a major opportunity for innovation. Bag et al.(2023) argued that such integrations could radically transform decision-making, making it more data-driven and secure (Bag et al. 2023). Regarding supply chains, the implementation of IoT blockchain systems is likely to ensure synchronous compliance and optimize various processes, according to Pajooh et al. (2022) (Honar Pajooh et al. 2022).

This article has theoretical implications as it explores how blockchain technology could be applied to decentralized and assured data-sharing systems. Beyond affirming prior research findings regarding blockchain efficiency in scalability and security, it generates new hypotheses regarding the integration of AI and sophisticated algorithms. Haddad et al. (2022) emphasized that their synergistic use could permanently alter conventional data management patterns (Haddad et al. 2022). Furthermore, this study anticipates that blockchain will remain a key enabler, shaping various industries by providing transparency, accountability, and innovation. Such assumptions align with recent efforts in blockchain research and application, highlighting the necessity of continuous investigation.

This discussion demonstrates the critical role of blockchain technology in addressing data-sharing issues. This study is valuable not only for verifying existing knowledge but also for providing opportunities for theoretical and practical advancements by describing the current capabilities of the subject, outlining the interactions of its elements, and projecting its future evolution. These contributions support the further development of interdisciplinary

studies to harness the potential of blockchain systems in securing and enhancing data-sharing processes.

6. Conclusion

The article posits that the implementation of blockchain is the primary strategic tool for secure data sharing in healthcare, finance, and supply chain management. By addressing core issues such as scalability, latency, and data integrity, blockchain provides a unique platform for enabling modern digital environments. The evidence presented demonstrates that blockchain technology can optimize work processes and improve both the efficiency and security of operations across various sectors. Utilizing consensus mechanisms and fraud detection algorithms, the reliability and robustness of blockchain systems have been shown to enhance efficiency in several studies under diverse challenging scenarios. It is crucial to make blockchain engineers aware of the domain-specific requirements they are working in.

In the healthcare industry, blockchain has numerous potential applications due to its strong merits in data privacy and interoperability, which enhance patient care and increase organizational efficiency. In the financial industry, blockchain not only eliminates fraud but also enables efficient processing of transactional activities, thereby improving the sector's future structures. Similarly, in supply chain management, blockchain enhances traceability, provenance, and compliance, making it a strategic enabler of international trade.

While the results highlight the advantages of blockchain applications, they also indicate areas requiring further investigation. Future research should focus on the integration of blockchain with other emerging technologies such as IoT, artificial intelligence, and quantum computing. For example, combining blockchain with big data analytics could improve decision-making and predictive maintenance in financial and supply chains. Conversely, integrating blockchain with IoT could transform real-time monitoring and compliance for large systems.

Therefore, it is promising to assert that blockchain represents a breakthrough foundational technology that can establish an efficient and secure framework for data sharing. However, its further development is necessary and requires additional investigation into its full potential, including scalability, interoperability, and compliance with governmental regulations.

Thus, the research presented here outlines possibilities for further exploration and aims to inspire the practical application of blockchain as a foundational technology for the digital world.

References

Aldoubaee, A., Hassan, N., & Rahim, F. (2023). A Systematic Review on Blockchain Scalability. *International Journal of Advanced Computer Science and Applications,* 14 (9). https://doi.org/:10.14569/ijacsa.2023.0140981

Bag, S., Rahman, M. S., Gupta, S., and Wood, L. C. (2023). Understanding and predicting the determinants of blockchain technology adoption and SMEs' performance. *The International Journal of Logistics Management,* 34 (6), 1781-1807. https://doi.org/:10.1108/IJLM-01-2022-0017

Bellucci, M., Cesa Bianchi, D., and Manetti, G. (2022). Blockchain in accounting practice and research: systematic literature review. *Meditari Accountancy Research,* 30 (7), 121-146. https://doi.org/:10.1108/MEDAR-10-2021-1477

Fiore, M., Capodici, A., Rucci, P., Bianconi, A., Longo, G., Ricci, M., Sanmarchi, F., et al. (2023). Blockchain for the Healthcare Supply Chain: A Systematic Literature Review. *Applied Sciences*, 13 (2). https://doi.org/:10.3390/app13020686.

Ghadge, A., Bourlakis, M., Kamble, S., and Seuring, S. (2023). Blockchain implementation in pharmaceutical supply chains: A review and conceptual framework. *International Journal of Production Research,* 61 (19), 6633-6651. https://doi.org/:10.1080/00207543.2022.2125595

Haddad, A., Habaebi, M. H., Islam, M. R., Hasbullah, N. F., and Zabidi, S. A. (2022). Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems. *IEEE Access,* 10, 94583-94615. https://doi.org/:10.1109/ACCESS.2022.3201878

Honar Pajooh, H., Rashid, M. A., Alam, F., and Demidenko, S. (2022). Experimental Performance Analysis of a Scalable Distributed Hyperledger Fabric for a Large-Scale IoT Testbed. *Sensors*, 22 (13). https://doi.org/:10.3390/s22134868.

Leng, J., Zhou, M., Zhao, J. L., Huang, Y., and Bian, Y. (2022). Blockchain Security: A Survey of Techniques and Research Directions. *IEEE Transactions on Services Computing,* 15 (4), 2490-2510. https://doi.org/:10.1109/TSC.2020.3038641

Lohmer, J., Ribeiro da Silva, E., and Lasch, R. (2022). Blockchain Technology in Operations & Supply Chain Management: A Content Analysis. *Sustainability*, 14 (10). https://doi.org/:10.3390/su14106192.

Mamun, A. A., Azam, S., and Gritti, C. (2022). Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction. *IEEE Access,* 10, 5768-5789. https://doi.org/:10.1109/ACCESS.2022.3141079

Manogaran, G., Alazab, M., Shakeel, P. M., and Hsu, C. H. (2022). Blockchain Assisted Secure Data Sharing Model for Internet of Things Based Smart Industries. *IEEE Transactions on Reliability,* 71 (1), 348-358. https://doi.org/:10.1109/TR.2020.3047833

Miah, A., Rahouti, M., Jagatheesaperumal, S. K., Ayyash, M., Xiong, K., Fernandez, F., and Lekena, M. (2023). Blockchain in Financial Services: Current Status, Adoption Challenges, and Future Vision. *International Journal of Innovation and Technology Management,* 20 (08), 2330004. https://doi.org/:10.1142/S0219877023300045

Mu, K., and Wei, X. (2023). EfShard: Toward Efficient State Sharding Blockchain via Flexible and Timely State Allocation. *IEEE Transactions on Network and Service Management,* 20 (3), 2817-2829. https://doi.org/:10.1109/TNSM.2023.3236433

Nayyer, N., Javaid, N., Akbar, M., Aldegheishem, A., Alrajeh, N., and Jamil, M. (2023). A New Framework for Fraud Detection in Bitcoin Transactions Through Ensemble Stacking Model in Smart Cities. *IEEE Access,* 11, 90916-90938. https://doi.org/:10.1109/ACCESS.2023.3308298

Neene, V., Ng'uni, A., Jere, B., Kalunga, P., and Phiri, M. (2022). Blockchain Technology and its Implication for the Financial Sector in Zambia. *Zambia ICT Journal,* 6 (1), 52-60. https://doi.org/:10.33260/zictjournal.v6i1.139

Ponsam, J. G., Duvvuri, S., and Roy, S. (2023). Electronic Healthcare Management System Using Blockchain Technology. *2023 International Conference on Circuit Power and Computing Technologies (ICCPCT),* 10-11 Aug. https://doi.org/:10.1109/ICCPCT58313.2023.10245668.

Qasim, N. H., Al-Helli, H.I., Savelieva, I., Jawad, A. M. (2023). Modern Ships and the Integration of Drones – a New Era for Marine Communication. *Development of Transport,* 4 (19). https://doi.org/:10.33082/td.2023.4-19.05

Qasim, N. H., Jumaa, D. A., Rahim, F., Jawad, A. M., Khaleefah, A. M., Zhyrov, G., and Ali, H. (2024). Simplifying IP multimedia systems by introducing next-generation networks with scalable architectures. *Edelweiss Applied Science and Technology,* 8 (4), 2042-2054. https://doi.org/:10.55214/25768484.v8i4.1580

Qasim, N. H., Rahim, F., and Bodnar, N. (2024). A comprehensive investigation of an LTE-enabled smart door system using the Arduino UNO. *Edelweiss Applied Science and Technology,* 8 (4), 697-708. https://doi.org/:10.55214/25768484.v8i4.1446

Qasim, N. H., Vyshniakov, V., Khlaponin, Y., and Poltorak, V. (2021). Concept in information security technologies development in e-voting systems. *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS),* 3 (9), 40-54.

Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., Sonkamble, R. G., et al. (2023). Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. *Sustainability*, 15 (8). https://doi.org/:10.3390/su15086337.

Sazu, M. H., and Jahan, S. A. (2022). Impact of blockchain-enabled analytics as a tool to revolutionize the banking industry. *Data Science in Finance and Economics,* 2 (3), 275-293. https://doi.org/:10.3934/DSFE.2022014

Sharma, P., Namasudra, S., Chilamkurti, N., Kim, B.-G., and Crespo, R. G. (2023). Blockchain-Based Privacy Preservation for IoT-Enabled Healthcare System. *ACM*

Trans. Sen. Netw., 19 (3), Article 56. https://doi.org/:10.1145/3577926

Van Nguyen, T., Cong Pham, H., Nhat Nguyen, M., Zhou, L., and Akbari, M. (2023). Data-driven review of blockchain applications in supply chain management: key research themes and future directions. *International Journal of Production Research,* 61 (23), 8213-8235. https://doi.org/:10.1080/00207543.2023.2165190

Wang, Z., and Guan, S. (2023). A blockchain-based traceable and secure data-sharing scheme. *PeerJ Comput Sci,* 9, e1337. https://doi.org/:10.7717/peerj-cs.1337

Wei, X., Yan, Y., Guo, S., Qiu, X., and Qi, F. (2022). Secure Data Sharing: Blockchain-Enabled Data Access Control Framework for IoT. *IEEE Internet of Things Journal,* 9 (11), 8143-8153. https://doi.org/:10.1109/JIOT.2021.3111012

Xue, L., Liu, D., Huang, C., Shen, X., Zhuang, W., Sun, R., and Ying, B. (2022). Blockchain-Based Data Sharing With Key Update for Future Networks. *IEEE Journal on Selected Areas in Communications,* 40 (12), 3437-3451. https://doi.org/:10.1109/JSAC.2022.3213312

Yousif, O., Dawood, M., Jassem, F. T., and Qasim, N. H. (2024). Curbing crypto deception: evaluating risks, mitigating practices and regulatory measures for preventing fraudulent transactions in the middle east. *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico,* (22), 311-334. https://doi.org/:10.5281/zenodo.13732337