Vol. 08, No. 1 (2026) 251-262, doi: 10.24874/PES08.01.026

Proceedings on Engineering Sciences

www.pesjournal.net

ENHANCING INTEGRATED MANAGEMENT SYSTEMS THROUGH THE POTENTIAL APPLICATION OF BLOCKCHAIN TECHNOLOGY IN THE INTEGRATION OF QUALITY AND INFORMATION SECURITY

Ana Djokic[1]
Marija Zahar Djordjevic

Received 25.06.2025.
Revised 02.10.2025.
Accepted 23.10.2025.

Keywords:

Quality Management System, Information Security Management System, Integrated Management System, Blockchain Technology

A B S T R A C T

In modern business environments, establishing a clear and concise mechanism for harmonizing various management areas, such as quality management, environmental protection, occupational health and safety, risk management, and information security, is of great importance. A fragmented approach to different aspects of management brings numerous challenges. To achieve more efficient management, the concept of Integrated Management Systems (IMS) has been developed, based on connecting individual systems. This paper presents the theoretical foundations and models for the integration of Quality Management Systems (QMS) and Information Security Management Systems (ISMS). In addition to the analysis of the influential factors and challenges associated with integration, the focus of this work is on improving data security and integrity through the potential application of blockchain technology. Examples of practical application of blockchain-supported IMS in the healthcare sector, supply chain management, and the management of academic and institutional documents illustrate the benefits, including improving information infrastructure security and the preserving of data integrity within IMS. The qualitative results obtained by reviewing existing literature on this topic and the comparative analysis of IMS with and without blockchain support show that this technology has the potential to significantly enhance the integration of management systems, but also that there are numerous challenges related to implementation costs, scalability and regulatory frameworks.

1. INTRODUCTION

Various management systems, such as Quality Management Systems (QMS; International Organization for Standardization [ISO], 2015a), Environmental Management Systems (EMS; ISO, 2015b), Occupational Health and Safety Management Systems (OHSAS 18001; British Standards Institution [BSI], 2007; ISO, 2018a), Risk Management (RM; ISO, 2018b), Information Security Management Systems (ISMS; ISO, 2013), and others, are still often implemented in isolation by many organizations today, as separate systems, with

[1] Corresponding author: Ana Djokic
Email: ana.djokic@its.edu.rs

an emphasis on individual and specific business aspects. Considering the increasingly demanding and complex relationships between the market, regulatory bodies and stakeholders, this fragmented approach increasingly faces numerous challenges, in terms of less or insufficient efficiency, misalignment of objectives of different systems, duplication of tasks through parallel systems and an increase in administrative work. As a response to overcome and solve these problems, the concept of IMS has been developed, in which management systems are not viewed as independent elements, but as a single coherent framework (Manea, 2015). IMS can be defined as a unique set of interconnected processes that use common resources (human, infrastructural, informational, financial) in order to meet requirements, increase trust, and minimize non-compliance of all interested parties (Karapetrović, 2003). This systemic approach, from the perspective of ISO standards, enables organizations to strategically align individual management systems through better coordination and communication between different parties, as well as optimiziation of external and internal audits. In this way the organization becomes more flexible and better prepared for the development and introduction of new standards. In addition, IM unites the interdependencies between quality, environmental and health protection, and information security, and thus enable comprehensive, harmonized and enhanced risk management and improved regulatory compliance (Karapetrović, 2003).

Despite the advantages of IMS and the evident progress in its development and application, it is important to emphasize that there is no single international standard that defines it in detail. Organizations are thus faced with a lack, but also with an opportunity, to align various certification and regulatory requirements based on consensus practices from existing standards (ISO, 2013, 2015a, 2015b, 2018a, 2018b; BSI, 2007) and adapt them to their own needs and strategic goals (Manea, 2015).

Considering the intensive development of digital technologies, new opportunities for improvement of IMS are opening up. Blockchain, as a decentralized and immutable database, enables transparent, secure, and permanent recording of all key processes and events within an organization (Joannou et al., 2020; Saberi et al., 2019; Wang et al., 2023). These characteristics are particularly important in the context of IMS, where trust in data integrity and traceability is essential for compliance with standards and effective risk management (Casino et al., 2019; Joannou et al., 2020). The integration of blockchain technology into IMS can significantly improve information security, increase process transparency, and facilitate collaboration between different stakeholders, wuth raising the level of trust and operational efficiency (Al-Emari et al., 2022; Owolabi & Owolabi, 2025).

The aim of this paper is to explore, through the analysis of the theoretical models and practical examples, the possibilities and challenges of integrating QMS and ISMS within IMS, with a special focus on the potential application of blockchain technology in improving information security, transparency and data integrity. Special attention is paid to identify advantages and limitations of this approach, as well as to the prospects of its application in sectors with high demands for quality and security, such as healthcare (Careline & Godhavari, 2022), supply chain management (Byreddy, 2025) and the management of academic and institutional documents (Zhang et al., 2018).

This paper presents a qualitative analysis of the influential factors on various management areas in the process of integrating QMS and ISMS systems, based on the literature (Fiore et al., 2021; Luma & Abazi, 2019). Also, a critical analysis of the relevant existing literature was conducted, identifying research gaps in the field of IMS. Based on this analytical framework, hypotheses were formulated and further discussed in the paper. Finally, the paper shows a comparative analysis of IMS integration with and without the application of blockchain technology, highlighting the potential advantages, limitations and perspectives for the further development of this approach.

2. INTEGRATION OF QUALITY AND INFORMATION SECURITY MANAGEMENT SYSTEMS WITHIN AN INTEGRATED MANAGEMENT SYSTEM

2.1 Reasons for integration

Along with the growth and development of digital infrastructure in organizations, there is a growing need for new systems that would integrate information security with other management systems. Thanks to IMS, organizations have gained the opportunity to align individual management components with their clearly defined objectives (Manea, 2015). Given that QMS and ISMS have overlapping objectives and mutually complementary operational processes, their integration within IMS contributes to a comprehensive improvement of organizational performance through structured management, risk management, and regulatory compliance. This minimizes duplication of resources and simplifies monitoring and auditing tasks (Manea, 2015). Integrated QMS-ISMS enable organizations to jointly address risks related to quality and security, because the processes that ensure product or service quality are closely related to information security. IMS is a tool for overcoming problems, such as conflicting objectives in isolated systems, which results in operational efficiency of the organization (Daneshjo et al., 2021). Integrated risk management across business processes enables better preventive measures and timely response to potential security risks and errors, which results in strengthening the resilience of the organization and a culture of trust between all stakeholders (Fiore et al., 2021).

2.2 Models and frameworks for the integration of quality and information security management systems

A systematic approach, which is essential for the successful integration of QMS and ISMS, is often implemented in practice through the application of maturity models. These models serve as frameworks for analyzing organization's readiness to implement integration and enable analysis of the development level of critical management elements. The aspects they cover relate to identifying priority development areas in accordance with the organization's vision and goals, as well as defining, documenting and standardizing workflows. This improves consistency, monitoring and control of activities within the IMS. Also, an important segment is the assessment of employee competencies, as well as the evaluation of technical and technological support that enables efficient system integration (Karapetrović, 2003).

The integration maturity model identifies several levels, from the isolated implementation of individual management systems, through partial coordination and process alignment, to a fully integrated and functionally aligned management system. Through this model, organizations analyze the current level of integration and plan the development of higher levels of interoperability and efficiency. In addition to their analytical role in assessing the level of integration, maturity models are also used to support the strategic planning of management system integration. Their application enables the identification of key integration elements. This includes establishing a unified documentation system, harmonizing procedures for internal and external audits and defining a common performance measurement system. Such system enables unified monitoring of quality and security aspects in accordance with the requirements of individual management systems. By identifying these elements, process rationalization, reduction of operational risks and improvement of overall organizational efficiency are achieved (Komadinić & Majstorović, 2017).

A case study of an educational institution specializing in exam organization found in its research that the integration of QMS and ISMS results in the unification of internal control procedures, joint planning and implementation of employee training, as well as the definition of integrated key performance indicators that enable unified performance monitoring in the areas of quality and information security. Improvements were achieved in the domains of more efficient use and optimization of resources, increased transparency, and better compliance with regulatory requirements (Daneshjo et al., 2021).

In terms of relevant ISO standards, the integration of QMS and ISMS contributes to their harmonization, especially through ISO 9001 and ISO/IEC 27001 (ISO, 2015a; ISO, 2013). These standards require coordination of common work areas, such as risk management, documentation control, implementation of internal audits, and processes for continuous improvement. In that context, ISO 9004 is used as an upgrade for the strategic development of the organization, with an emphasis on long-term stability, adaptability and improvement of management processes (ISO, 2018c).

2.3 Influencing factors and challenges

For the successful implementation of QMS and ISMS integration, it is essential to consider and understand the various factors that influence the implementation, as well as the challenges and limitations that could potentially threaten the sustainability of such an IMS (Daneshjo et al., 2021; Luma & Abazi, 2019). Different influencing factors, from technical and organizational, through organizational culture factors to managerial factors, as well as potential challenges, are presented in Table 1.

Table 1. Influencing factors and limitations in the integration of QMS and ISMS

Management Area	Critical requirements and operational challenges
Human Resources	Competencies, awareness and commitment of employees; importance of training and development of integrated skills
Resources and Infrastructure	Costs, technology, and professional staff
Organizational Culture	Resistance to change, fostering collaboration and continuous education
Change Management	Strategy for accepting changes and adopting new practices
Management and Leadership	Clearly defined management structures, roles, responsibilities, support from management structures, effective communication
Technical Interoperability	Integration of different IT tools and systems, careful planning and coordination

A qualitative analysis of the influencing factors on various management areas in the process of QMS and ISMS integration, derived from (Fiore et al., 2021; Luma & Abazi, 2019) is presented in Figure 1.

Although maturity models and research results based on real implementations indicate clear advantages of QMS and ISMS integration, in practice, isolated management of these systems is still often applied. This is mainly due to a lack of competencies and capacities within organizations themselves, resistance to change and a lack of tools that enable management encompassing all relevant processes (Fiore et al., 2021; Luma & Abazi, 2019).

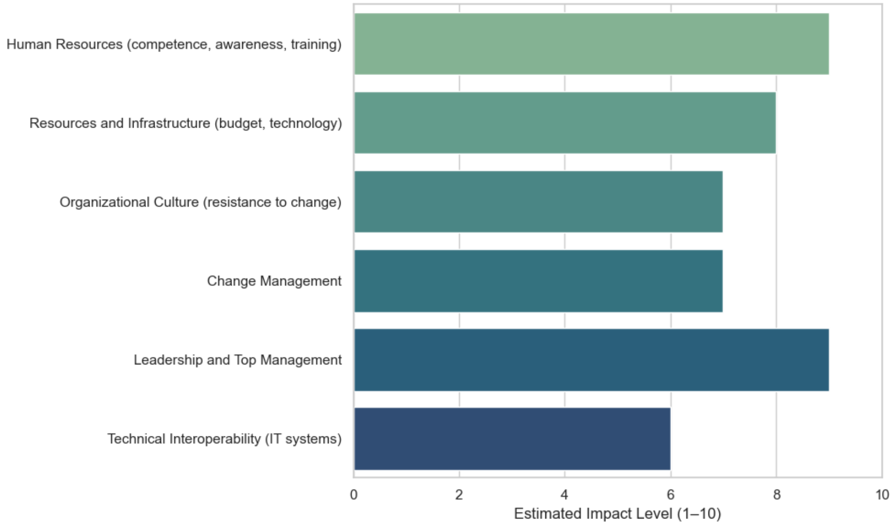

Figure 1. Factors influencing various management areas

In that context, there is space for exploring the potential of modern digital technologies, such as blockchain, which can contribute to improving the reliability and operational efficiency of IMS through decentralized control, data verification and immutability of records.

3. POTENTIAL APPLICATIONS OF BLOCKCHAIN TECHNOLOGY IN INTEGRATED MANAGEMENT SYSTEMS

3.1 Basic characteristics of blockchain technology

Blockchain technology represents a decentralized, immutable and transparent mechanism for recording, storing and verifying data, which has the potential to significantly enhance the functionality of IMS (Saberi et al., 2019). Decentralization eliminates the need for a central entity, thereby increasing system resilience through the equitable exchange of data among network participants, which contributes to a higher degree of security and reliability. Immutability ensures that data and transactions, once recorded, remain permanently stored and that there is a continuous record of all changes, which is essential for transparency and compliance with management system requirements and standards (Joannou et al., 2020).

3.2 Potential application of blockchain technology in enhancing information security and quality management systems

Thanks to its fundamental principles, blockchain technology represents an effective approach for improving information infrastructure security and preserving data integrity within an IMS environment. The immutable record of this technology enables permanent and verifiable recording of all events, which is crucial for demonstrating compliance with relevant standards and audit processes (Heng et al., 2017). Automated recording of access, changes and approvals contributes to a higher degree of accountability and transparency in information management, while enhanced traceability provides a clear and continuous overview of data flow, from source to end-user. These features help reduce the risk of internal abuses and external manipulations (Joannou et al., 2020).

The application of blockchain technology in secure data sharing systems enables the implementation of controlled, permission-based access, which minimizes the risk of unauthorized information disclosure and improves operational efficiency (Al-Emari et al., 2022). Furthermore, the integration of blockchain into cybersecurity strategies encourages the development of decentralized defense architectures that reduce vulnerabilities characteristic of centralized systems. Contemporary research confirms the effectiveness of this technology in improving intrusion detection systems, particularly through the protection of event logs and enhanced real-time threat management (Owolabi & Owolabi, 2025).

In the context of QMS, the transparency and immutability of blockchain technology significantly enhance documentation and verification processes. This technology enables the creation of confidential and trustworthy records of certificates, quality-related documents and audit trails, which contribute to increased trust among all stakeholders. Additionally, transparent record-keeping reduces the possibility of fraud, thus further strengthening trust and supporting compliance with regulatory requirements, particularly in sectors where traceability and quality integrity are key success factors (Casino et al., 2019).

3.3 Application Examples

3.3.1 Blockchain technology in the healthcare sector

The healthcare sector represents one of the most promising areas for the application of blockchain-supported IMS, primarily due to the combined requirements for high standards of service quality and rigorous information protection measures. The integration of QMS and ISMS in this domain is becoming increasingly important due to the sensitivity of patient data and the complexity of the regulatory framework that includes regulations, such as the Health Insurance Portability and Accountability Act (HIPAA; U.S. Department of Health and Human Services, 1996) and the General Data Protection Regulation (GDPR; International Data Protection Regulation, 2016) (Careline & Godhavari, 2022).

Blockchain technology enables the formation of distributed and immutable electronic health record (EHR) databases, thereby ensuring the preservation of information integrity, transparency and controlled access to data by authorized actors (Careline & Godhavari, 2022). Such an architecture contributes to compliance with data protection standards and simultaneously strengthens the principles of continuous improvement in the quality of healthcare services.

Advanced applications in this area include the integration of blockchain with artificial intelligence (AI) based platforms, enabling automated data processing, predictive analytics and more efficient management of healthcare processes. Technologies based on smart user support systems, using data verified by blockchain mechanisms, enable simpler appointment scheduling, more precise symptom tracking and timely advice, while preserving the confidentiality and security of health information (Patel et al., 2024).

Although current implementations of blockchain technology are predominantly limited to prototype phases and pilot projects tested under controlled conditions, the results indicate its potential to overcome the fragmentation of information systems in healthcare and encourage the establishment of a unified, decentralized infrastructure for data management (Owolabi & Owolabi, 2025). The main advantages include increasing accountability of stakeholders, reducting administrative barriers and improving processes traceability, which is in line with IMS requirements (Owolabi & Owolabi, 2025; Careline & Godhavari, 2022; Azaria et al., 2016).

Current literature shows that most successful initiatives refer to functional models or limited case studies, while full operational implementation is still in the development phase (Careline & Godhavari, 2022; Patel et al., 2024). Nevertheless, the analysis of existing research and theoretical frameworks clearly confirms the significant contribution of blockchain technology to the improvement of IMS in the healthcare sector, especially in the areas of data protection, regulatory compliance and increasing overall process efficiency (Owolabi & Owolabi, 2025; Careline & Godhavari, 2022; Patel et al., 2024; Azaria et al., 2016).

3.3.2 Blockchain technology in integrated supply chains

The integration of blockchain technology with Enterprise Resource Planning (ERP) systems and Internet of Things (IoT) devices brings significant improvements in the area of quality management and data security within supply chains. Blockchain enables the establishment of immutable and transparent records of product origin, which contributes to compliance with relevant quality and safety standards throughout the entire supply process (Byreddy, 2025).

Connecting real-time IoT data with blockchain ledgers allows for efficient product traceability, confirmation of their authenticity and increases the accountability of all involved stakeholders. These features reduce the risk of counterfeiting and illicit activities, while simultaneously facilitate organizations' fulfillment of regulatory requirements and enhance transparency towards stakeholders (Khan et al., 2024).

Pilot projects combining blockchain and IoT technologies in the healthcare supply chains demonstrate how logistical processes can be simplified and made more transparent. Such solutions provide greater visibility and trust among all participants, which is especially important for the distribution of sensitive and high-value medical products, while improving quality control and data security (Nanda et al., 2023).

Based on the analysis of existing literature, there is a recognized need for a greater number of empirical studies that would examine not only the technological aspects, but also the socio-economic and organizational consequences of the introduction of blockchain into complex supply chains (Saberi et al., 2019; Kshetri, 2018; Peshattiwar et al., 2025; Khan et al., 2024; Byreddy, 2025).

3.3.3 Blockchain technology in academic and institutional document management

The scientific and research community recognizes the significant potential of the blockchain technology in improving document management, especially in the context of ensuring the integrity, availability and validity of academic records. Traditional systems for verifying diplomas, transcripts, and other documents often face challenges such as the possibility of forgery, limited traceability and insufficient transparency. In this context, blockchain enables the creation of distributed, immutable records that provide reliable validation of information, thereby strengthening academic integrity and optimizing administrative processes (Zhang et al., 2018).

One of the latest examples of advanced blockchain-based solutions in higher education is a pilot project developed at the Polytechnic Faculty in Kutaraja (Banda Aceh). In that study, the authors present the development and evaluation of a prototype system for academic document management, with the aim of increasing the security, transparency and efficiency of the diploma and related document verification process. The results of the implementation show that blockchain architecture significantly reduces the risk of forgery, speeds up authenticity checks and fosters a higher degree of trust of all stakeholders in the academic data management process. Most of the surveyed users from the pilot phase reported an increased sense of security, as well as improved availability and efficiency of the system, compared to previous methods. Still, the solution is in the testing and evaluating phase, without full institutional integration, which points to the need for further empirical verification under real, everyday faculty working conditions (Mirnawati et al., 2024).

4. PERSPECTIVES, CHALLENGES AND DEVELOPMENT DIRECTIONS OF INTEGRATED MANAGEMENT SYSTEMS WITH BLOCKCHAIN TECHNOLOGY

4.1 Contemporary trends and challenges in blockchain integration into integrated management systems

The further development of IMS increasingly relies on connecting blockchain technology with advanced digital solutions such as AI, the IoT and Big Data analytics. In this context, AI contributes to improving the analysis and interpretation of data recorded in blockchain networks, enabling timely anomaly detection and predictive risk management, while IoT sensors allow the continuous real-time collection of operational data, which can be directly integrated into the IMS environment (Yu, 2024).

The implementation of smart contracts opens up possibilities for deeper automation of workflows, especially regarding the verification of compliance with internal and external standards. This reduces the need for manual checks, accelerates process flow, and decreases the probability of errors. In addition, real-time analysis provides further support for decision making, providing organizations with more flexible and proactive management of key quality and safety aspects in a complex IMS environment (Patel et al., 2024).

The IMS structured in this way has the potential for further improvements through the introduction of hybrid blockchain models and new consensus mechanisms, which create opportunities for more efficient integration into large and complex systems (Peshattiwar et al., 2025). Simultaneously, previous experiences in QMS and ISMS standardization can serve as a basis for integration with distributed ledger technologies (Bernardo et al., 2015).

Finally, the vision for the development of IMS increasingly relies on the principles of trust, transparency and accountability, through the construction of management models that meet the needs of the digital age and emphasize inclusivity and ethical sustainability of the system.

For responsible and inclusive implementation, it is necessary to develop management models based on the principles of trust, transparency and accountability, which will consider the interests of all stakeholders and ensure the ethical sustainability of the integrated systems (Owolabi & Owolabi, 2025).

4.2 Challenges in implementing blockchain in IMS

The implementation of blockchain technology in IMS faces a series of technical, operational and organizational challenges, as shown in Table 2.

Table 2. Overview of challenges and limitations in the potential application of blockchain technology in IMS

Challenges and Limitations	Description	Source
Technical Limitations	Scalability limitations, transaction processing delays, and integration and processing costs make it difficult to introduce blockchain into large, legacy IMS, especially in real-time and in industries with complex processes.	Geetha et al., 2024 Peshattiwar et al., 2025;
Interoperability	Harmonization of different data formats, protocols and business workflows between IMS and blockchain networks requires technical adaptation and additional investment.	Mane et al., 2024
Regulatory Challenges	Reconciling transparency and privacy is demanding, especially due to regulations on confidential data protection and insufficient number of clear legal frameworks.	Saberi et al., 2019; Mane et al., 2024
User Requirements	The development of reliable, stable infrastructures and intuitive user interfaces is necessary, because the end-users find it difficult to accept new technology.	Geetha et al., 2024

Table 2. Overview of challenges and limitations in the potential application of blockchain technology in IMS (continued)

Challenges and Limitations	Description	Source
Organization and Culture	Resistance to change, lack of blockchain experts and the complexity of managing and coordinating among stakeholders hinder successful integration.	Haughton et al., 2023; Owolabi & Owolabi, 2025
Financial Aspects	High initial investments, maintenance costs and the need to hire professional personnel can be detrimental to sustainability and return on investment	Peshattiwar et al., 2025
Ethical and Social Consequences	There are issues of equal access to information, the potential for deepening existing inequalities and challenges related to user privacy protection.	Owolabi & Owolabi, 2025
Environmental Challenges	There can be high energy consumption in some blockchain models, the need for energy-efficient protocols and reducing environmental impact.	Sahadevan & Mishra, 2024

Multidisciplinary collaboration and continuous adaptation of the regulatory and organizational framework are necessary in order to balance the benefits of modern innovations with the recognized risks and limitations of the technology.

4.3 Critical analysis of existing literature and identification of research gaps

To systematize existing research approaches and identify relevant gaps in the literature, Table 3 presents an overview of relevant works dealing with the application of blockchain technology in IMS.

Table 3. Overview of key works on the application of blockchain technology in IMS and related systems

Source	Research Focus	Main Contributions	Limitations / Gaps
Azaria et al., 2016	Blockchain for medical data management	Decentralized access and data authorization, Interoperability	Prototype level, without full implementation
Zhang et al., 2018	Blockchain for clinical data sharing	FHIRChain for secure and scalable data exchange in healthcare	Focus only on healthcare data and protocols
Manea, 2015	ISMS within the IMS Framework	Description of ISMS integration as part of IMS, potential for blockchain integration	No concrete examples of blockchain integration
Joannou et al., 2020	Permitted blockchain in systems engineering	Solutions for access control and data immutability throughout the system lifecycle	Focus on systems engineering, not IMS by standards
Al-Emari et al., 2022	Blockchain in Intrusion Detection Systems (IDS)	Detailed overview of blockchain integration in IDS for increased security	Limited to IDS, no broader IMS application
Careline & Godhavari, 2022	Blockchain in health records and insurance	Secure, interoperable data exchange with smart contracts	Focus only on healthcare IMS
Owolabi & Owolabi, 2025	Blockchain in healthcare information systems	Security, interoperability, and privacy in healthcare systems	Limited to the healthcare sector
Patel et al., 2024	Integration of AI and blockchain in healthcare IMS	Automation and advanced analytics with AI and blockchain	Lack of real-world implementations
Peshattiwar et al., 2025	Blockchain in the supply chain	Hybrid blockchain models, AI smart contracts, energy efficiency	Focus on the supply chain, less directly on IMS integration
Byreddy, 2025	Blockchain in the pharmaceutical supply chain	Analysis of SAP blockchain solutions for authentication and transparency	Focus exclusively on the supply chain

Based on the presented works, it is possible to identify several key research gaps that limit the further development of a holistic concept for blockchain-supported IMS. Previous research predominantly focuses on individual segments of the system (e.g. medical data, security, supply chains) and offers solutions for specific challenges, while comprehensive blockchain-based IMS models are poorly developed or in their infancy. There is a lack of an integrated approach to unify multiple subsystems (quality, information security, environmental protection) within a single blockchain framework. Most works remain at the level of theoretical models or pilot implementations, which limits the practical validation of the results and their usability in complex real-world IMS environments. There is a pronounced gap between theoretical potentials and extensive empirical evidence in everyday business practice. Due to the absence of standardized frameworks and clearly defined regulatory guidelines for integrating blockchain into IMS, broader and systemic application of such solutions is hindered. Issues related to privacy, energy-efficient protocols and the broader social impact of blockchain within IMS are still insufficiently explored, although they are increasingly recognized as key factors for sustainability and development.

4.4 Proposed research framework and hypotheses

In order to overcome the identified gaps, this paper proposes the development of a research framework that encompasses the functional integration of QMS and ISMS elements in IMS supported by blockchain technology, to enhance integrity, reliability and transparency. The framework is further upgraded by integrating modern technologies such as AI and IoT, with the aim of improving the analysis and integration of various digital data sources. The proposed framework should enable the evaluation of compliance with international standards, enhance data security and integrity and assess the operational and environmental sustainability of the IMS. Based on the established framework hypotheses are proposed, as shown in Table 4.

Table 4. Research hypotheses

Label	Formulation	Explanation
H1	The integration of blockchain technology into IMS significantly increases data security and integrity compared to traditional IMS approaches.	Decentralized and immutable blockchain architecture reduces the risk of data manipulation and unauthorized access, thereby increasing the level of trust of all users in the system.
H2	The application of smart contracts within an IMS reduces administrative errors and accelerates compliance processes.	Automation of verification and control through smart contracts minimizes the possibility of human error and shortens process handling time.
H3	The use of blockchain supported by AI and IoT technologies enhances the efficiency of quality and safety management within an IMS.	Combination of blockchain, AI analytics and IoT sensors enables real-time monitoring, anomaly detection, and efficient management of operational risks and quality.
H4	The existence of standardized regulatory frameworks positively influences the acceptance and implementation of blockchain-based IMS solutions.	A clear legal and regulatory framework reduces uncertainty, increases stakeholder trust, and encourages the readiness of companies and institutions to adopt innovative IMS models.
H5	The development of energy-efficient blockchain protocols contributes to the sustainability of IMS without compromising performance.	Energy-optimized protocols conserve energy resources and ensure the long-term sustainability of IMS implementation in a digital environment.

The formulated hypotheses represent a logical framework for the comparative analysis of existing literature on IMS solutions with and without the use of blockchain technology, and serve as a starting point for evaluating the achievements, limitations and potential identified in relevant research papers.

5. COMPARATIVE ANALYSIS OF INTEGRATED MANAGEMENT SYSTEMS WITH AND WITHOUT THE APPLICATION OF BLOCKCHAIN

IMS utilizing blockchain technology demonstrate significantly greater operational efficiency compared to traditional approaches. This is achieved by reducing process redundancy and simplifying data flow, while automated controls and immutable records significantly enhance risk management. Conversely, classic IMS often rely on fragmented and manually intensive processes, which limit timely response and precise compliance monitoring, especially in sectors with strict regulations such as the pharmaceutical industry (Byreddy, 2025; Daneshjo et al., 2021).

The application of blockchain technology also brings significant improvements in data security and integrity, providing immutable records and a high level of traceability. The distributed network minimizes the risks of compromise that centralized systems cannot fully eliminate, thereby increasing the trust of all stakeholders. This level of security and transparency aligns with modern requirements for responsible management and data integrity (Geetha et al., 2024; Saberi et al., 2019).

However, the financial aspects and scalability of blockchain solutions present challenges that require careful analysis. High initial implementation costs, maintenance costs and energy consumption represent barriers to widespread adoption, while at the same time infrastructure is being improved for long-term sustainability. Traditional IMS have an advantage in ease of implementation and lower initial costs, but they face obsolescence in conditions where higher standards of security, transparency and interoperability are required (Imane et al., 2024; Peshattiwar et al., 2025).

Based on the presented differences in performance and characteristics of IMS with and without the application of blockchain technology, Table 5 provides a summarized overview of the main elements of the comparative analysis. This table clearly illustrates the advantages and disadvantages of both approaches, with a particular focus on data integrity, transparency, risk management, costs and system scalability.

Table 5. Comparative analysis of IMS with and without blockchain technology

Criterion	IMS without Blockchain	IMS with Blockchain
Data Integrity	Depends on centralized records, which can lead to data manipulation risks (Geetha et al., 2024; Saberi et al., 2019; Luma & Abazi, 2019)	Immutable and distributed ledger, high level of integrity and protection against manipulation (Peshattiwar et al., 2025; Saberi et al., 2019; Casino et al., 2019)
Process Transparency	Limited due to fragmented and manual processes, with weaker real-time visibility (Byreddy, 2025; Daneshjo et al., 2021; Fiore et al., 2021)	High, thanks to immutable records and real-time step-by-step tracking capabilities (Byreddy, 2025; Casino et al., 2019)
Risk Management	Fragmented, often reactive, without full system integration and control automation (Daneshjo et al., 2021; Patel et al., 2024; Manea, 2015)	Proactive and automated, with embedded smart contracts and real-time monitoring (Patel et al., 2024; Peshattiwar et al., 2025)
Audit Trail	Centralized records susceptible to manipulation or data loss, with a risk of inconsistency (Kshetri, 2018; Saberi et al., 2019)	Immutable, transparent and accessible records of all transactions, facilitating tracking and control (Casino et al., 2019; Saberi et al., 2019)
Initial Implementation Costs	Lower initial costs, simpler implementation based on existing systems (Manea, 2015; Komadinić & Majstorović, 2017)	Higher initial costs due to infrastructure requirements and specific resources (Imane et al., 2024; Peshattiwar et al., 2025)
Scalability	More flexible models with existing standards and lower technical requirements (Komadinić & Majstorović, 2017; Fiore et al., 2021)	Limitations in throughput and scalability, but energy-efficient protocols are being developed to overcome challenges (Peshattiwar et al., 2025; Sahadevan & Mishra, 2024)
Standard Compliance	Greater compliance with existing ISO standards (ISO 9001, ISO 14001, ISO 27001) as IMS traditionally rely on them (Bernardo et al., 2015; Manea, 2015)	Need for further development and continued alignment of blockchain solutions with international standards (Fiore et al., 2021; Imane et al., 2024)
Security and Data Protection	Depends on the security of centralized systems, often vulnerable to attacks and data breaches (Luma & Abazi, 2019; Kshetri, 2018)	Greater security through decentralization, cryptographic protection and transparent access management (Casino et al., 2019; Saberi et al., 2019)
Sustainability and Energy Efficiency	Lower resource requirements, generally more energy-efficient (Manea, 2015; Komadinić & Majstorović, 2017)	Higher energy requirements, but with a growing focus on energy-optimized protocols (hybrid models) to reduce negative effects (Peshattiwar et al., 2025)

The diagram in Figure 2 presents a comparative analysis of the performance of IMS with and without the application of blockchain technology across six key criteria: security, transparency, efficiency, costs, scalabilit, and compliance.

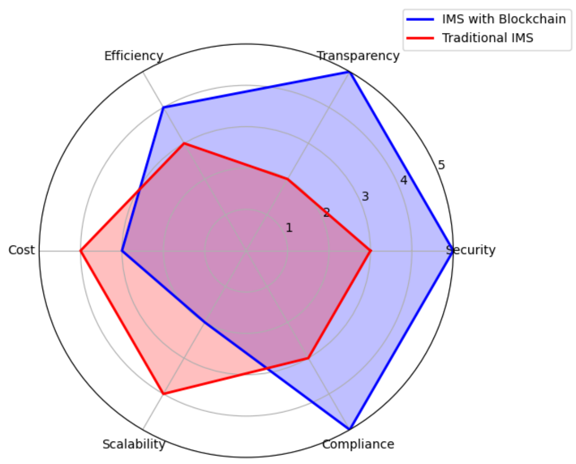

Figure 2. Performance of IMS systems with and without the application of blockchain technology

It is evident that IMS with blockchain achieve significantly better results in the areas of security, transparency, efficiency and compliance, confirming their superiority in risk management and data integrity.

On the other hand, traditional IMS show an advantage in terms of costs and scalability, where blockchain solutions still face challenges, particularly due to higher initial investments and limited network throughput. This visual representation clearly illustrates the balance between the benefits and challenges of blockchain integration into IMS, highlighting areas for further research and improvement.

6. CONCLUSION

IMS represent a crucial tool for coordinated and efficient management of various business aspects, such as quality, information security, environmental protection and risk management. This paper analyzed the complexity of their integration, with a special focus on connecting QMS and ISMS. Through a review of theoretical models and practical examples, it was determined that IMS enable better integration of resources and processes, reduce redundancies and improve compliance with international standards.

Particular attention was paid to the potential application of blockchain technology as an innovative tool for enhancing the security, integrity and transparency of data within the IMS framework. The analysis of practical examples from various sectors, including healthcare, supply chain management, and academic and institutional document management, showed that blockchain brings significant improvements in terms of immutability of records, decentralization, and process automation, which further strengthens stakeholder trust and operational efficiency.

However, significant challenges related to the implementation of blockchain technology in IMS were also identified, particularly in the areas of high initial costs, scalability issues, energy efficiency and regulatory ambiguities. These challenges require a multidisciplinary approach to research and development, as well as the definition of clear legal and standardization frameworks.

The proposed research framework and the hypotheses set in the paper open perspectives for further empirical research and testing of blockchain integration into IMS, with the aim of realizing and quantifying the expected benefits, as well as developing effective solutions for overcoming existing obstacles.

In conclusion, the integration of IMS with blockchain technology offers significant opportunities for improving management systems in the digital age, but the success of its application will depend on a holistic approach that encompasses technical, organizational, regulatory and ecological aspects, where continuous research and practical implementations play a key role.

References:

Al-Emari, S., Anbar, M., Sanjalawe, Y. K., Manickam, S., & Hasbullah, I. (2022). Intrusion detection systems using blockchain technology: A review, issues and challenges. *Computer Systems Science and Engineering, 40*(1), 36–50. https://doi.org/10.32604/csse.2022.017941

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, October). MedRec: Using blockchain for medical data access and permission management [Paper presentation]. In *Proceedings of the 2nd International Conference on Open and Big Data (OBD), Boston, MA, USA*. https://doi.org/10.1109/OBD.2016.11

Bernardo, M., Simon, A., Tarí, J. J., & Molina-Azorín, J. F. (2015). Benefits of management systems integration: A literature review. *Journal of Cleaner Production, 94*, 260–267. https://doi.org/10.1016/j.jclepro.2015.01.075

British Standards Institution [BSI] (2007). *Occupational health and safety management systems – Requirements (OHSAS 18001:2007)*. London, UK: BSI.

Byreddy, M. R. (2025). Blockchain integration in pharmaceutical supply chain management: An analysis of SAP's enterprise solution. *Journal of Computer Science and Technology Studies, 7*(4), 786–791. https://doi.org/10.32996/jcsts.2025.7.4.91

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

Careline, L. G. S., & Godhavari, T. (2022). Implementation of electronic health record and health insurance management system using blockchain technology. *International Journal of Advanced Computer Science and Applications (IJACSA), 13*(6). http://dx.doi.org/10.14569/IJACSA.2022.0130679

Daneshjo, N., Malega, P., Kóňa, J., & Barilová, B. (2021). Integrated management system and corporate risk management. *TEM Journal, 10*(4), 1686–1693. https://doi.org/10.18421/tem104-2

Fiore, A. P. A., Facin, A. L. F., & Muniz, J., Jr. (2021). Information security and quality management systems integration: Implementation in an institution specialized in exams organization. In *Proceedings of the 2nd South American International Conference on Industrial Engineering and Operations Management* (pp. 430–441). Sao Paulo, Brazil: IEOM Society International. https://doi.org/10.46254/SA02.20210231

Geetha, R., Vijayanandh, T., Ananthi, S. N., & Mercilin Raajini, X. (2024, August). Enhanced cybersecurity: Development and evaluation of a secure data sharing paradigm based on blockchain technology [Paper presentation]. In *2024 First International Conference on Electronics, Communication and Signal Processing (ICECSP)*. https://doi.org/10.1109/ICECSP61809.2024.10698576

Haughton, O., Campbell, C., Walcott, T. H., & Neaga, I. (2023, December 14–15). Blockchain-based supply chain management systems: A systematic mapping study of academic research. In *Proceedings of the 2023 International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA), Zagreb, Croatia*. https://doi.org/10.1109/10384965

Heng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress)* (pp. 557–564). Honolulu, HI, USA: IEEE. https://doi.org/10.1109/JPROC.2017.2787104

International Data Protection Regulation. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L119, 1–88. https://gdpr-info.eu

International Organization for Standardization [ISO] (2013). *Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013)*. Geneva, Switzerland: ISO.

International Organization for Standardization [ISO] (2015a). *Quality management systems – Requirements (ISO 9001:2015)*. Geneva, Switzerland: ISO. https://www.iso.org/standard/62085.html

International Organization for Standardization [ISO] (2015b). *Environmental management systems – Requirements with guidance for use (ISO 14001:2015)*. Geneva, Switzerland: ISO. https://www.iso.org/standard/60857.html

International Organization for Standardization [ISO] (2018a). *Occupational health and safety management systems – Requirements with guidance for use (ISO 45001:2018)*. Geneva, Switzerland: ISO. https://www.iso.org/standard/63787.html

International Organization for Standardization [ISO] (2018b). *Risk management – Guidelines (ISO 31000:2018)*. Geneva, Switzerland: ISO. https://www.iso.org/standard/65694.html

International Organization for Standardization [ISO] (2018c*). Quality management — Quality of an organization — Guidance to achieve sustained success (ISO 9004:2018).* Geneva, Switzerland: ISO. https://www.iso.org/standard/70397.html

Joannou, D., Kalawsky, R., Martínez-García, M., Fowler, C., & Fowler, K. (2020). Realizing the role of permissioned blockchains in a systems engineering lifecycle. *Systems, 8*(4), 41. https://doi.org/10.3390/systems8040041

Karapetrović, S. (2003). Musings on integrated management systems. *Measuring Business Excellence, 7*(1), 4–13. https://doi.org/10.1108/13683040310466681

Khan, H. U., Khan, M. A. R., & Ali, F. (2024). Systematic mapping study of blockchain integrated supply chain management. *Security and Communication Networks, 2024*, Article ID 8884339. https://doi.org/10.1155/2024/8884339

Komadinić, V. R., & Majstorović, V. D. (2017). Maturity model of integrated management system. *International Journal Advanced Quality, 45*(3), 47–50. https://doi.org/10.25137/IJAQ.n3.v45.y2017.p47-50

Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

Luma, A., & Abazi, B. (2019). The importance of integration of information security management systems (ISMS) to the organization's enterprise information systems (EIS). In *Proceedings of the 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1205–1208). Opatija, Croatia: MIPRO. https://doi.org/10.23919/MIPRO.2019.8756645

Imane, L., Noureddine, M., Driss, S., & Hanane, L. (2024). Towards blockchain-integrated enterprise resource planning: A pre-implementation guide. *Computers, 13*(1), 11. https://doi.org/10.3390/computers13010011

Manea, C. A. (2015). Information security management - Part of the integrated management system. *Acta Universitatis Cibiniensis, 66*(1), 102–107. https://doi.org/10.1515/aucts-2015-0036

Mirnawati, Z., Aini, Z., & Khair, R. (2024). Implementing blockchain for secure and efficient academic document management. *Indonesian Journal of Computer Science, 13(6), 9343–9349*. https://doi.org/10.33022/ijcs.v13i6.4502

Nanda, S. K., Panda, S. K., & Dash, M. (2023). Medical supply chain integrated with blockchain and IoT to track the logistics of medical products. *Multimedia Tools and Applications, 82*, 32917–32939. https://doi.org/10.1007/s11042-023-14846-8

Owolabi, B. O., & Owolabi, F. A. (2025). Blockchain-powered health innovation information systems for secure, interoperable, and privacy-preserving healthcare data management. *International Journal of Science and Research Archive, 15*(2), 1629. https://doi.org/10.30574/ijsra.2025.15.2.1629

Patel, S., Waghmare, O., Kumbhar, R., Bhadange, A., & Charkha, S. (2024). HealthSphere: Integrated AI-powered and blockchain based health management and support system. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 4*(1), 101. https://doi.org/10.48175/IJARSCT-22616

Peshattiwar, A. A., Mohanraj, P., Gerald, A., & Dharmalingam, S. (2025). Blockchain technology in supply chain management: Prospects and challenges for implementation. *ITM Web of Conferences, 76*, 02007. https://doi.org/10.1051/itmconf/20257602007

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research, 57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

Sahadevan, V. K., & Mishra, U. (2024). Blockchain-enabled integrated three-layer bio-circular economy model with wastewater treatment, emissions, and controlled cheese spoilage. *Journal of Industrial and Production Engineering, 42*(4), 385–405. https://doi.org/10.1080/21681015.2024.2424827

U.S. Department of Health and Human Services. (1996). *Health Insurance Portability and Accountability Act of 1996.* Preuzeto sa https://www.hhs.gov/hipaa/index.html

Wang, S. L., Zhang, Y., Sheng, X., & Luo, X. Y. (2023). Blockchain in supply chain collaboration: A quantitative study. *International Journal of Simulation Modelling*, *22*(3), 532-543. https://doi.org/10.2507/IJSIMM22-3-CO15

Yu, H. (2024). Exploring enterprise information security management and risk assessment through big data and the Internet of Things. *Journal of Computational Methods in Sciences and Engineering, 25*(2), 1519–1534. https://doi.org/10.1177/14727978241300787

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. *Computational and Structural Biotechnology Journal, 16*, 267–278. https://doi.org/10.1016/j.csbj.2018.07.004

Ana Djokic
Information Technology School,
Zemun,
Serbia;
Faculty of Engineering,
University of Kragujevac,
Kragujevac,
Serbia
ana.djokic@its.edu.rs
ORCID 0009-0002-3469-586X

Marija Zahar Djordjevic
Faculty of Engineering,
University of Kragujevac,
Kragujevac,
Serbia
maja_199@yahoo.com
ORCID 0000-0003-4905-2728