RESEARCH PAPER

Emerging Trends in Blockchain-Assisted Internet of Medical Things: A Bibliometric Review

Aditi Sharma[1], Rajesh Kumar Kaushal[1]* and Naveen Kumar[1]

[1]*Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India*
[1]*Aditi.sharma@chitkara.edu.in,* [1]*Rajesh.kaushal@chitkara.edu.in and* [1]*Naveen.sharma@chitkara.edu.in*

Received: 14th June, 2026; Revised: 20th July 2026; Accepted: 20th August, 2026; Available Online: 05th September 2026

ABSTRACT

The intersection of blockchain and the Internet of Medical Things (IoMT) has sparked a new wave of research on securely managing healthcare data while ensuring privacy and security. This paper addresses the key challenge of ensuring data security and transparency in IoMT systems. This study aims to provide a bibliometric analysis of research on blockchain and IoMT by analysing publications listed in the Scopus database between 2019 and 2025. A total of 177 publications were analyzed using bibliometric techniques and visualization tools such as R and VOSviewer. The analysis addresses the patterns of publication, country contributions, networks of collaboration, keyword co-occurrence, and citation patterns, as well as emerging research themes. The results suggest that there is a significant amount of research interest in blockchain-based IoMT, and India and China are leading countries in the study of blockchain-based IoMT, with India's research collaborations with other countries being strong. The top research topics revealed by the keyword analysis are blockchain, IoT, IoMT, healthcare, security, data privacy, and digital storage, indicating a growing focus on secure data exchange in healthcare and decentralized management of medical information. It also indicates ongoing issues in terms of scalability, interoperability, computational demands, energy efficiency, and real-time processing. From these research trends, lightweight consensus mechanisms, efficient cryptographic solutions, and standardized interoperability solutions are identified as potential areas for further research. The study offers a framework to understand the research site of blockchain–IoMT and prioritizes research gaps that can facilitate secure, scalable, and interoperable healthcare systems.

Keywords: Blockchain; Smart contract; IoMT; Internet of Things; Electronic Health Records; Decentralized System

How to cite this article: Sharma A, Kaushal RK, Kumar N., Emerging Trends in Blockchain-Assisted Internet of Medical Things: A Bibliometric Review. Int J Drug Deliv Technol. 2026; 16(8): 262-277. DOI: 10.25258/ijddt.16.8.27
Source of support: Nil.
Conflict of interest: None

1. INTRODUCTION

Healthcare has become a digital world, leading to the connection between electronic health records (EHRs), remote patient monitoring systems, and networked healthcare services. These technologies help healthcare professionals acquire, analyze, and share different types of patient data in real time, both within the clinical and organizational context. The implementation of connected medical devices, in particular, has given rise to the expansion of healthcare data beyond the traditional clinical record to include continuously collected physiological measurements, diagnostic data, and other patient-related data. This digitalisation, which can facilitate timely clinical decision-making and enhance the availability of patient data, contains extensive challenges concerning secure data management, maintaining the privacy of the data, data integrity, and the efficient exchange of healthcare data between various stakeholders [1]. As data flows from digital devices, healthcare data has grown, demanding the development of technological structures that can support a secure, scalable, and trustworthy healthcare environment.

The IoMT takes healthcare digitalization one step further by enabling medical devices, wearable sensors, monitoring systems, and other connected healthcare technologies that collect and share information continuously. The IoMT distributed environment presents a number of challenges for healthcare data management. Healthcare data can flow through various devices, networks, and organizational levels, making it critical to ensure its security and privacy [2]. Interoperability across heterogeneous devices and healthcare systems is also a challenge, as data can be created and stored on different platforms. Moreover, as more data is generated from medical IoT devices, issues of scalability, real-time processing, and storage, especially when handling large and complex medical data sets. The challenges emphasize the need for secure and scalable methods that can enable reliable and secure exchange of information, while preserving the integrity and availability of healthcare information. The potential of blockchain technology to solve the challenges of trust, security, and data management in IoMT-based healthcare environments has risen. It is a distributed system that can provide decentralized trust among various healthcare organisations along with blockchain[3].

**Author for Correspondence: Aditi.sharma@chitkara.edu.in*

Blockchain technology has gained a lot of research interest as a solution to overcome some of these challenges in IoMT-based healthcare systems. Its distributed design allows entities participating in the network to keep their records in a verifiable manner without having to rely on a central authority. Controlled access to sensitive healthcare information can be achieved by blockchain-based authorization mechanisms, and cryptographically linked transactions can enable data integrity and traceability [4]. Smart contracts can also handle pre-defined authentication, authorization, consent, and data sharing conditions. These features have encouraged researchers to explore the potential benefits of blockchain and IoMT for enhancing trust, security, transparency, and accountability in healthcare data management [5].

While these are seeming benefits, blockchain-IoMT integration is not a cure-all for technological and operational challenges. While blockchain networks demand activities and consensus, computation, and maintenance of the distributed ledger, IoMT environments feature resource-constrained devices and constantly generated diverse data [6]. Due to this, scalability, transaction latency, computational overhead, energy consumption, interoperability, privacy, and efficient data management remain key factors shaping the real-world adoption of blockchain-based IoMT applications. The literature has thus progressed from traditional blockchain-based secure environments to other technology solutions that are designed to enhance the efficiency, intelligence, and scalability of connected healthcare environments.

In recent years, researchers have dedicated their efforts to the field of IoMT, leading to a growing number of publications that focus on the technology's blockchain applications. The present research includes various aspects, including secure information exchange, smart contracts, interoperability, secure authentication, access control, privacy preservation, and healthcare data security, as shown in Figure 1. Research into the development of scientific publications, prominent contributors, geographical distribution, collaboration networks, citation links, and the development of key research topics is also important [7]. Bibliometric analysis offers an objective method to analyse these aspects and can help to illustrate the intellectual and conceptual landscape of a developing research field.

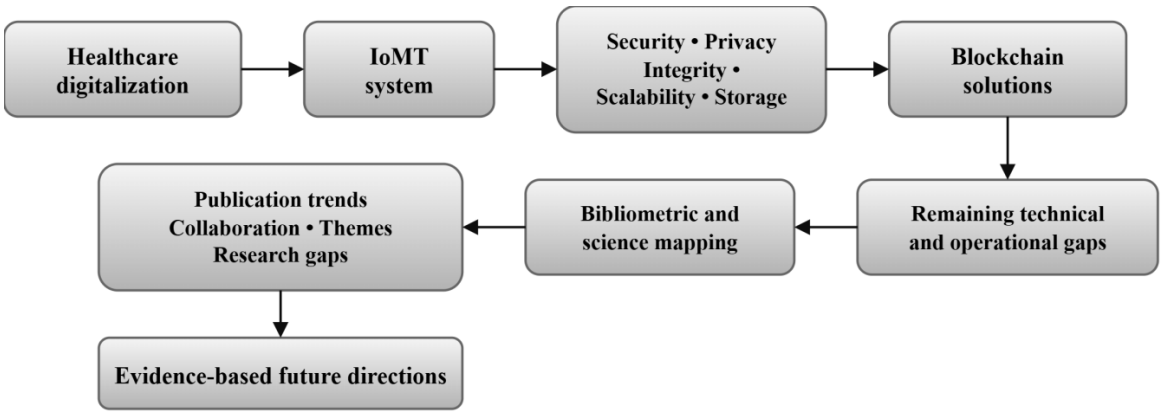


Figure 1. Conceptual motivation and scope of the present study

Although blockchain-related and healthcare research have been studied using bibliometric methods, there is a need for an in-depth analysis of blockchain-IoMT research to gain insight into its research development, collaborative structures, and emerging trends. Taking the example of research priorities, in particular, it can be seen that the technological problems that are still getting high-priority attention, and those that are under-explored, are gaining insights [8]. Based on this, the present study provides a bibliometric analysis of the research on the blockchain-based IoMT literature from publications obtained from the Scopus database [9]. The bibliometric and science-mapping research methods are used to analyse trends in publications, geography of contributions, research collaboration, citation patterns, and keyword relationships. The scientific and conceptual structure of the field and the main research themes are visualized by using VOSviewer, and the bibliometric analysis of the field is conducted in R. The study not only analyzes the productivity of the publications, but also aims to investigate how the thematic development of blockchain–IoMT research has changed, what problems it has faced that continue, and what potential directions it may take in the future.

The following are the major contributions of this study:

To explore the development and evolution of blockchain in IoMT research by leveraging publication and citation analysis.

To highlight the most important countries, authors, institutions, and sources of publication that play a significant role in this research field.

To explore scientific co-authorship and citation networks as well as co-citation and related networks of intellectual relationships.

To emphasize persistent research challenges and see possible directions for future development of secure,

scalable, and interoperable blockchain-based IoMT systems.

Blockchain Technology and Its Relevance to IoMT

Blockchain technology is a distributed system for recording, verifying, and distributing transactions among nodes in a network. In contrast to a traditional, centralized system where data is managed and controlled from a single source, blockchain operates with a shared ledger where verified transactions are data that is synchronised among the authorized participants on the network. The information is recorded in blocks, and cryptographic hash functions create logical connections between the blocks [10]. Participating nodes agree about the validity and ordering of transactions they are submitting to the ledger by applying certain rules of validation and consensus. Furthermore, smart contracts can be used to automate certain rules and conditions, allowing for regulated and transparent interactions with other users on the network. The decentralization, cryptographic verification, consensus, immutability, and programmability of blockchain have extended the scope of its use beyond cryptocurrency. These are especially important for healthcare and IoMT applications, where data is created and shared across various devices, medical staff, and institutions.

2.1 Blockchain Architecture and Transaction Workflow

A blockchain network is a group of nodes that are linked together and collaborate to create, validate, and keep the blockchain updated. A network participant begins a transaction and sends it to the network for verification. However, transactions are confirmed based on predetermined rules and a consensus mechanism, depending on the blockchain architecture. Transactions are then combined and added to the ledger, leaving a sequential and transparent history of network operations. Cryptographic hashing makes the information recorded and can help detect unauthorised changes to the information [11]. The typical workflow of a transaction is to initiate a transaction, propagate it to the other nodes that need to participate in it, validate it, agree or authorize it, and commit it to the distributed ledger. While specific implementation steps vary between blockchain platforms, these steps all ensure agreement on valid transactions and consistency amongst all nodes [12]. In healthcare applications, these can facilitate traceable interactions between patients, healthcare professionals, institutions, and integrated medical systems.

A blockchain transaction follows a series of steps as shown in Figure 2—initiation, broadcast, consensus—before it is added to a block and becomes part of the distributed ledger. Each block is cryptographically linked to the previous one, ensuring a historical record of transactions can be verified. The multiple copies of the ledger on the various nodes create a level of consistency and remove dependence on a single point of control. Together, these mechanisms provide the foundational support for data integrity, traceability, and accountability in blockchain-based systems [13]. These properties are especially important in healthcare and IoMT applications since data is created and shared between various devices, healthcare professionals, and organizations, and it is essential to ensure that data-related transactions are accurately verified and tracked.

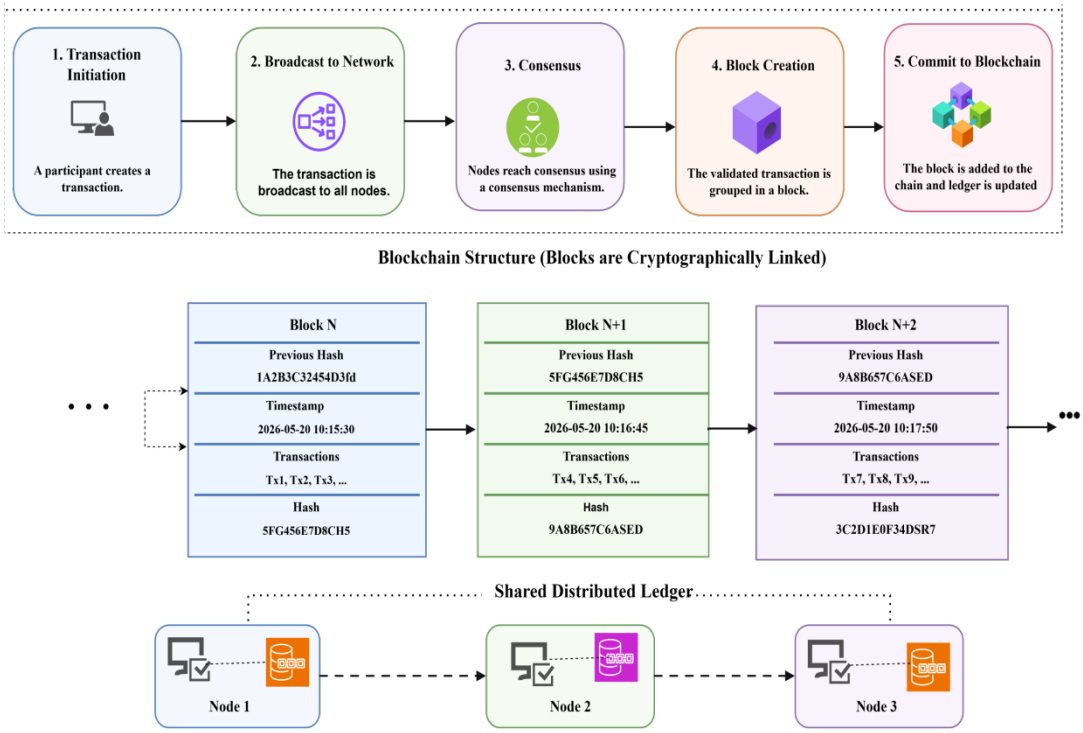


Figure 2. Operational flow of transaction processing in a blockchain network

2.2 Types of Blockchains and Their Suitability for IoMT

Based on participation, governance, and access control, blockchain networks can be categorized into four types: public, private, consortium, and hybrid. In general, public blockchains offer access to anyone and are highly transparent, while private blockchains have limited access for only authorized entities and offer better organizational control [14]. Healthcare environments consisting of multiple hospitals, labs, diagnostic centers, and other parties are allowed to participate in consortium blockchains, which are established for collaboration within a group of organizations. Hybrid blockchains offer a combination of public and private properties and may be viewed as a form of semi-transparent blockchain that still offers the opportunity to protect sensitive data [15]. For IoMT applications, where medical data is sensitive and could be shared with multiple authorized parties, it is crucial to choose an appropriate blockchain model. Public architectures are more open and decentralized, while permissioned and consortium architectures offer more controlled participation and identity management, with configurable access strategies [16]. For this reason, the right blockchain solution for IoMT applications will be determined by aspects of privacy, scalability, transaction speed, governance, interoperability, and the number of healthcare organizations involved.

Table 1. Comparison of different types of blockchains

Feature	Public	Private	Consortium	Hybrid
Participation	Open	Restricted	Selected organizations	Both
Governance	Distributed	Single organization	Multiple organizations	Both
Identity	Pseudonymous	Known	Known	Configurable
Data visibility	High	Restricted	Controlled	Selective
Access control	Limited	Strong	Strong	Configurable
Scalability	Dependent	Higher	Higher	Dependent
Healthcare suitability	Limited for sensitive data	Suitable	Highly relevant to multi-organisation	Dependent

Table 1 shows that blockchain types differ in decentralization, transparency, governance, privacy, and access control. While public blockchains offer increased transparency and decentralization, private and consortium blockchains allow for more controlled access and participation while also protecting sensitive data. In healthcare and IoMT settings, medical data often flows through various authorized parties, and privacy and transparency are a priority [17]. Confidentiality and accountability are vital in healthcare and IoMT environments, where medical information is shared among different authorized individuals. So, choosing a blockchain architecture should depend on the needs of the applications, such as its governance, its scalability, its access-control requirements, and its transaction performance.

2.3 Blockchain–IoMT Integration in Healthcare

By combining blockchain with IoMT, the system aims to create a secure and verifiable environment for exchanging health data, leveraging the power of connected devices and blockchain technology. Health IoMT devices such as wearables, remote monitoring systems, and other devices generate healthcare data constantly [18]. Blockchain is not an infrastructure replacement for IoMT, but rather an additional capability to offer connected healthcare environments mechanisms for the integrity, traceability, authentication, and controlled sharing of information among authorized parties. Smart contracts are another feature that enhances the functionality of blockchain-based IoMT systems by automatically fulfilling specific rules that are preprogrammed within a blockchain network. These standards can help with authorization, authentication, access control, and controlled data exchange in the healthcare industry [19]. This can enable patient interactions with healthcare providers, institutions, and the devices they connect with, and keep track of authorized transactions.

However, there are a few challenges with the integration of blockchain into IoMT. While IoMT environments are often resource-constrained devices that produce large volumes of mixed healthcare data, blockchain operations can impose further demands on computational, communication, storage, and transaction processing. The important research challenges are thus scalability, latency, energy usage, privacy protection, and real-time processing. The constraints have inspired researchers to explore lightweight consensus mechanisms, artificial intelligence, federated learning, and other complementary methods for data storage in blockchain-facilitated IoMT systems.

2. RELATED BIBLIOMETRIC STUDIES AND RESEARCH GAP

The combination of blockchain with the IoMT has generated significant research interest because of the growing need for security, privacy, and data management in healthcare environments. Previous research has focused on various aspects of blockchain-enabled IoMT, such as secure healthcare data sharing, authentication and access control, privacy preservation, intelligent healthcare applications, decentralized storage, and system performance. Instead of looking into these developments individually, a review of the literature can be carried out in

the context of the main technological trends that have influenced the development of studies related to the Internet of Things and blockchain.

3.1 Existing Studies on Blockchain-Enabled IoMT

Medical devices generate and transmit patient data in a distributed network, which is the nature of IoMT, making security and privacy one of the most widely studied challenges in blockchain-based IoMT. Previous research has focused on how blockchain can enhance authentication, data integrity, provide privacy for data exchange, and ensure verifiable and tamper-proof records of healthcare transactions. This suggested a blockchain-based privacy-preserving authentication scheme for IoMT that allows for decentralized authentication without relying on a third-party trusted authority. They showed that blockchain-based authentication systems could enhance the protection of privacy and resistance to common security attacks in medical-device systems [20]. Likewise, another study examined the security of IoMT systems using blockchain and emphasized that privacy, authentication, and integrity are key issues affecting the use of blockchains in connected healthcare[21].

To ensure the sharing of healthcare data among multiple parties and prevent information leakage, a mechanism based on blockchain that includes access control and privacy protection [22]. Smart contracts have also been used to restructure authorization policies and manage access to sensitive healthcare data. In recent research, smart-contract-based access-control mechanisms have proven to be useful in providing patient-centric data ownership, consent management, and fine-grained authorization while preserving an audit trail of data-healthcare interactions [23]. However, blockchain is not inherently privacy-proof, and problems with exposure of identities, vulnerability of smart contracts, computational power needs, and secure data exchange across organizations are still being studied.

One of the significant research fields is the combination of AI and federated learning with blockchain-based IoMT, which promises to enhance smart healthcare while maintaining patient privacy. Traditional machine-learning methods often rely on central data collection of health information, which can be difficult due to privacy, regulatory issues, and unauthorized disclosures [24]. Federated learning handles this by allowing models to be trained on the individual nodes in the distributed healthcare system, but only model parameters are shared, not the actual patient data. Still, federated-learning environments need to have some sort of trust-building protocol between the interacting entities, and verification of model updates, as well as a means to prevent malicious contributions.

In response, blockchain has been increasingly used with federated learning to overcome these challenges. A federated-learning framework based on blockchain was used to combine distributed learning to improve the security and privacy of healthcare IoT data against attacks [25]. Similarly, blockchain-based federated deep-learning methods are explored for securely sharing information and resisting attacks in healthcare IoT systems, which showcases the promise of decentralized trust and distributed learning [26]. This has been extended to successfully obtain EHR management in IoMT environments in other studies using decentralized federated learning and blockchain consensus mechanisms. While these methods decrease the need for centralized sharing of raw data, they still have a number of practical issues, including communication overhead, model aggregation, computational cost, scalability, convergence, and the limited resources found on IoMT devices.

Another key consideration in relation to the blockchain's application in healthcare is data storage, as the IoMT system can produce continuous sensor data, diagnostic information, electronic health records, and medical data. Keeping all healthcare data directly on the blockchain could lead to larger ledgers, higher storage demands, greater network overhead, and higher transaction costs.

Another study also presented a scalable healthcare architecture integrating blockchain with off-chain IPFS data storage to enhance healthcare data security and privacy. Here, direct data-storage needs on-chain were minimized via decentralized storage, and blockchain ensured trusted, tamper-resistant records were kept with healthcare information [27]. Moreover, decentralized EHR-sharing systems have implemented blockchain as a solution to address issues of privacy, scalability, and centralized storage, and have studied transaction latency, throughput, and failure rate. More recent blockchain-IoMT solutions have also used IPFS in addition to smart contracts to offer distributed storage, device enrolment, fault tolerance, and secure access to data [28]. Blockchain stores transaction data, transaction integrity proofs, authorization data, or content references, while larger healthcare-related documents remain stored in decentralized storage. However, there are some concerns with integrating blockchain with IPFS that come along with it, including data availability, encryption, key management, content persistence, privacy leakage, and performance with large-scale workloads in the IoMT. These are still significant challenges to the implementation of decentralized storage in healthcare.

While blockchain technology can enhance the trust and data integrity of IoMT systems, its scalability and performance are still significant challenges to its widespread healthcare adoption. IoMT systems include a huge number of heterogeneous and resource-limited devices that can produce continuous and time-sensitive information. However, blockchain could also add more overhead in terms of transaction validation, consensus, communication, computation, and storage. These requirements can affect latency, throughput, energy consumption, and real-time healthcare processing [29].

To address these challenges, recent work in the field of blockchain-IoMT has focused on lightweight

authentication, optimized communication, alternative consensus protocols, edge-assisted processing, and off-chain data handling. In practice, a two-phase blockchain-based IoMT system that leverages IPFS and smart contracts tests the performance of an IoMT system in terms of attack detection, energy consumption, throughput, packet delivery ratio, and latency. Similarly, other secure IoMT systems have tried to minimise the storage and computation space requirements whilst preserving privacy and authentication [30]. The other challenges discussed in reviews on the Healthcare use case of blockchain-IoT include scalability, interoperability, consent management, access control, latency, and resource constraints.

While some earlier works have discussed the applications of blockchain in healthcare and IoMT from the technological and review perspectives, this rapidly changing domain of IoMT. Some existing studies focus on blockchain-based healthcare while others focus on IoMT in general. The various studies have different coverage of the databases, time periods, scope, and approach. An updated bibliometric analysis of the literature on blockchain in IoMT can add further development of publications, significant papers, collaboration patterns, intellectual relationships, and the development of the key research themes. This analysis can also identify the ongoing and new research questions as well as evidence-based lines of future research.

Table 2. Comparison of previous review and bibliometric studies of the present research

Ref.	Year	Source/ duration	Scope	Tools/Method	Contribution	Limitations
[31]	2021	WoS, 626 documents (2016–2020)	Blockchain in healthcare	Bibliometric analysis; keyword co-occurrence	Publication growth, authors, countries, institutions, knowledge structure	Blockchain-enabled IoMT not investigated
[11]	2023	Literature, 73 selected papers (2017-2022)	Blockchain-based IoMT	Systematic review	Blockchain platforms, consensus, IoMT applications and challenges	Limited science-mapping and collaboration analysis
[15]	2024	182 articles (2018-2023)	Blockchain +IoMT	Systematic review +content analysis	Role and adoption of blockchain in IoMT	Content review rather than Scopus science mapping analysis
[17]	2024	Multiple databases (2019–2024)	Blockchain + IoMT privacy	PRISMA-based literature review	Privacy-preserving blockchain architectures and techniques	Privacy preservation rather than overall intellectual and thematic structure of blockchain-IoMT
[18]	2025	WoS, 545 articles (2019-2023)	Blockchain +e-healthcare	Bibliometrix R, VOSviewer, CiteSpace	Productivity, influential contributors, topics and emerging trends	Blockchain-enabled IoMT is not the exclusive analytical domain
[19]	2025	IoMT literature (2016–2023)	IoMT healthcare	Bibliometric/trend analysis	Development of IoMT, emerging technologies and healthcare applications	Focuses on IoMT; blockchain is one enabling technology rather than the central domain
Present Study	-	Scopus (2019-2025)	Blockchain enabled IoMT	Bibliometric analysis+ science mapping+ thematic analysis	Publication trends, contributors, collaboration networks, keyword relationships	Focused updated assessment of IoMT research

A comparative analysis of the existing studies is elaborated in Table 2, which indicates that blockchain-enabled health care has been analyzed from comprehensive bibliometric studies of blockchain in

health care to systematic reviews that focus on privacy and the adoption of technologies. Furthermore, the newly established concept of the domain is still evolving due to the quick development of AI, federated learning, decentralized data storage, smart contracts, and edge-supported healthcare. These developments inspire a new and relevant bibliometric analysis of the scientific evolution, collaboration patterns, intellectual connections, and emerging research topics of blockchain-enabled IoMT studies.

Therefore, the present study exploits the bibliometric performance analysis and science-mapping analysis on the Scopus-indexed articles to trace the research evolution of blockchain within the scope of IoMT and to reveal the dominant, emerging, and under-researched research paths.

3.2 Research Questions

The following research questions are established based on existing gaps found in the literature and are systematically studied in the present study in the field of blockchain-enabled IoMT research:

RQ1: What are the research areas that provide the conceptual framework of blockchain-enabled IoMT, and how are these interconnected in the current literature?

RQ2: Who are the most relevant authors, institutes, countries, and publications on blockchain-enabled IoMT research?

RQ3: How has blockchain been put in the context of IoMT research to solve the problem of data security, privacy, access control, data management, and decentralized storage in healthcare?

RQ4: What are the unsolved technological problems in the field of IoT research for blockchain-based solutions, and what research directions can be identified for future healthcare systems?

3. RESEARCH METHODOLOGY

A bibliometric research design is used to systematically review the scientific evolution and the intellectual structure of blockchain-based IoT research, which is named as “blockchain for the Internet of Medical Things”. Bibliometric analysis allows for the quantitative evaluation of scientific publications and can give information on the growth of publications, influential contributors, mode of cooperation, citation relations, and conceptual structure of a research field. Science-mapping techniques are used to visualize the relations between authors, countries, publications, sources, and research keywords, in addition to a performance analysis [32]. The methodological approach involves identifying and retrieving data, applying pre-established eligibility criteria, screening the retrieved data, cleaning and standardizing the data, performing bibliometric performance analysis, creating science maps, and interpreting the new research themes.

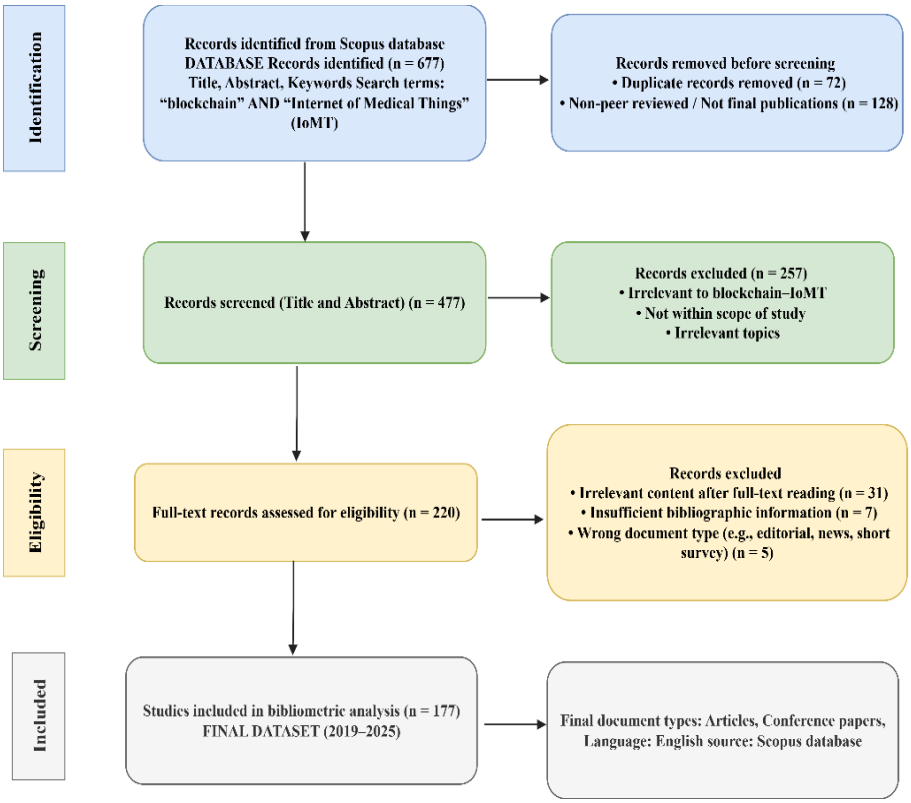


Figure 3. PRISMA flow diagram of the selection process

The process of selecting the studies is shown in Figure 3 was carried out systematically to ensure that the final data set would be consistent with the scope of the blockchain-enabled IoMT research. The retrieved records were then sequentially screened based on the pre-established criteria of publication time, type of document, language, and

relevance of the research field. After screening and applying the eligibility criteria, the chosen publications were the final data for subsequent bibliometric analysis. This is a systematic process for selection that makes the dataset used in the study more transparent and reproducible.

4.1 Data Source and Search Strategy

Scopus is the main bibliographic database used because it covers a wide range of publications from a large number of authors. The database offers structured bibliographic data needed for quantitative assessment and later analysis with science-mapping. Bibliometric methods are especially useful for analysing extensive scientific literature, as well as to reveal the intellectual and conceptual underpinnings of research [24].

A structured search strategy was used to find publications relevant to the study of blockchain for IoMT. The search was conducted on the title, abstract, and keyword fields, and Boolean operators were used to join the fundamental concepts of blockchain and the Internet of Medical Things[33]. The records were exported, containing bibliographic data necessary for further analysis. The retrieved publications were then screened and sorted according to the pre-designed screening and inclusion criteria to include the final dataset. Bibliometric tools enable systematic analysis of information like publications, author information, affiliations, citations, and other bibliographic relationships. Instead of defining keywords, a random search was performed to find relevant publications on the concepts. Boolean operators AND and OR are used to create various keyword combinations. TITLE-ABS-KEY (blockchain AND “Internet of Medical Things”) AND (LIMIT TO (AFFILCOUNTRY,“India”)) AND(LIMIT-TO (LANGUAGE,“English”))AND (EXCLUDE (PUBSTAGE, “aip")).

4.2 Inclusion and Exclusion Criteria

Predefined inclusion and exclusion criteria were used to retrieve the records from Scopus to make sure that the dataset is relevant and consistent. The selection criteria were carefully developed based on the aspect that was studied in this research article, the publication period, the language of the retrieved publications, the type of document, and the relevance of the publications to the study in the research article [34]. Studies were included if their title, abstract, or keywords showed a clear linkage between the applications of blockchain and healthcare using such IoMT solutions. Records that failed to meet scope and bibliographic criteria were not analyzed further.

Table 3. Inclusion and exclusion criteria for selection of publications

Criteria	Inclusion criteria	Exclusion Criteria
Research scope	Studies addressing blockchain in IoMT and healthcare	Studies unrelated to the integration of blockchain and IoMT
Language	Publication written in English	Language other than English
Subject relevance	Title, abstract, or keyword-based relevance to IoMT	Without relevance to the study objective
Publication status	Documents with sufficient bibliographic information	Incomplete records where bibliographic information was unavailable
Record quality	Records containing bibliographic information required	Records with insufficient or unusable bibliographic metadata
Duplication	Unique records retained for analysis	Duplicate records removed

The publications selected were based on a set of criteria that are summarized in Table 3. Application of these eligibility criteria allowed the final dataset to be kept within a specific scope on blockchain and IoMT and to provide bibliographic information for quantitative and network-based analysis. The eligible records after the screening process were then cleaned and standardized before bibliometric analysis.

4.3 Data Pre-processing and Bibliometric Analysis

The bibliographic data collected from Scopus were organized according to a systematic data pre-processing process. The bibliographic data were cleaned to ensure consistency in the information and reduce any errors that might affect subsequent network analysis. Duplication and inconsistencies were checked; institutional affiliation, country, source, and other bibliographic characteristics were harmonised as necessary.

Bibliometrix/Biblioshiny in R, as well as VOSviewer, were used for analysis of the cleaned bibliographic dataset. It offers an integrated platform for quantitative bibliometric analysis and science mapping, while Biblioshiny helps to explore bibliographic data interactively. The software VOSviewer was used to construct and visualize the bibliometric networks since it can handle the construction of bibliometric networks based on the relationships of co-authorship, co-citation, and keyword co-occurrence[24] .

Based on the bibliometric standards, it was divided into two complementary parts: performance analysis and science mapping. To evaluate the productivity and impact of the research domain, we used indicators including annual scientific output, key authors, contributing countries and institutions, relevant publication sources, and citation impact. The relational and intellectual structure of the literature was analysed using mapping techniques, such as co-authorship analysis, citation analysis, co-citation analysis, bibliographic coupling, and keyword co-occurrence analysis [34]. These methods allow systematic exploration of the quantitative development and knowledge structure underpinning

blockchain-based IoMT research. Finally, the bibliometric results were analysed to identify the collaboration patterns, new emerging technological trends, and the field that needs to be explored further.

5. RESULTS AND DISCUSSION

The bibliometric results give a quantitative and structural perspective of the evolution of blockchain-enabled IoMT research over the period studied. The analysis focuses on the trend of science production, geographical and scholarly contributions, the nature of research collaboration, citation relationships, and the conceptual structure of the research field. The data are analyzed in concert to understand the growth of the field and the research communities that contribute and influence its development.

5.1 Evolution of Blockchain-Enabled IoMT Research

Publications over time offer a preliminary quantitative growth and development of the field of blockchain-enabled IoMT. The annual scientific production in 2019–2025 is presented in Figure 4. The publication trend reflects the academic interest in the topic of blockchain and health internet systems during the study period. The observed development can be related to growing research interest in secure healthcare data exchange, decentralized trust, privacy preservation, and managing the data produced by interconnected medical devices.

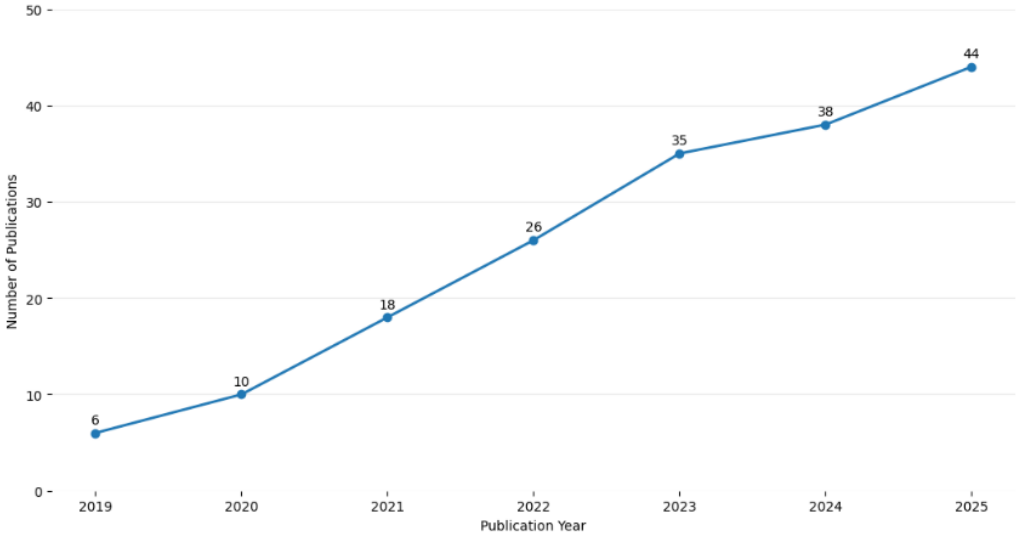


Figure 4. Annual scientific production in blockchain-enabled IoMT research

5.2 Geographical Contribution and Scientific Collaboration

The geographical distribution of the scientific production shows that the research on blockchain-enabled IoMT has generated interest from different parts of the world. The country-level analysis highlights the main contributors to the domain, as well as the geographical focus of research activity. The literature reviewed reveals that India is a strong contributor, with China and other countries showing considerable research interest.

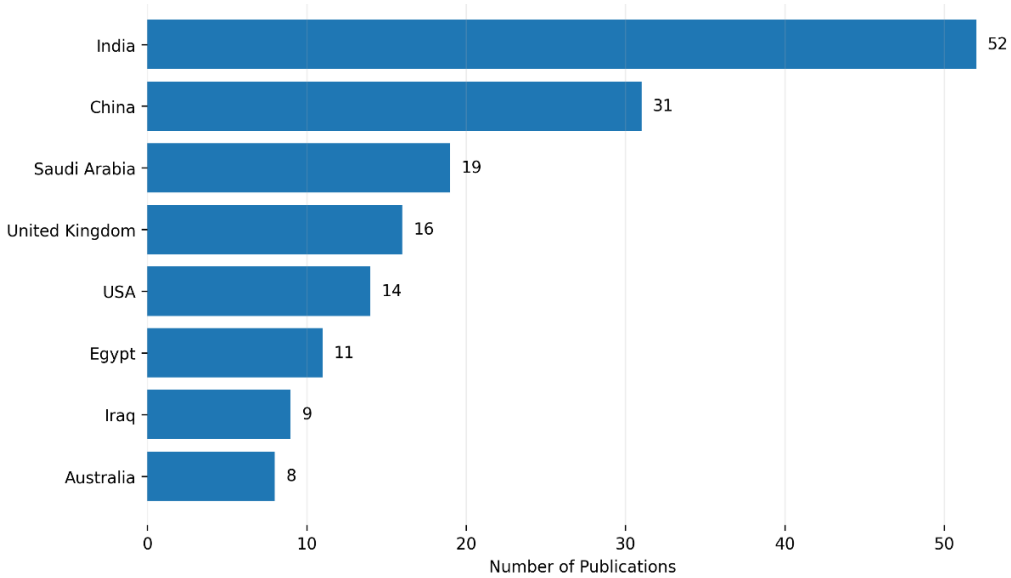


Figure 5 (a). Scientific production by country

A bibliometric network of global research collaborations and country-wise analysis is shown in Figure 5(a). This network diagram highlights India's pivotal position in international linkages. The links between nodes represent collaborative relationships among countries, while stronger link strength indicates a higher degree of research collaboration. The collaboration structure illustrates the linkages of India with other nations such as China, Saudi Arabia, and the UK, proposing that blockchain–IoMT research is being advanced in a transnational manner as opposed to single-national efforts. With prominent countries like China and India encouraging global information sharing, the network illustrates a globally integrated research environment.

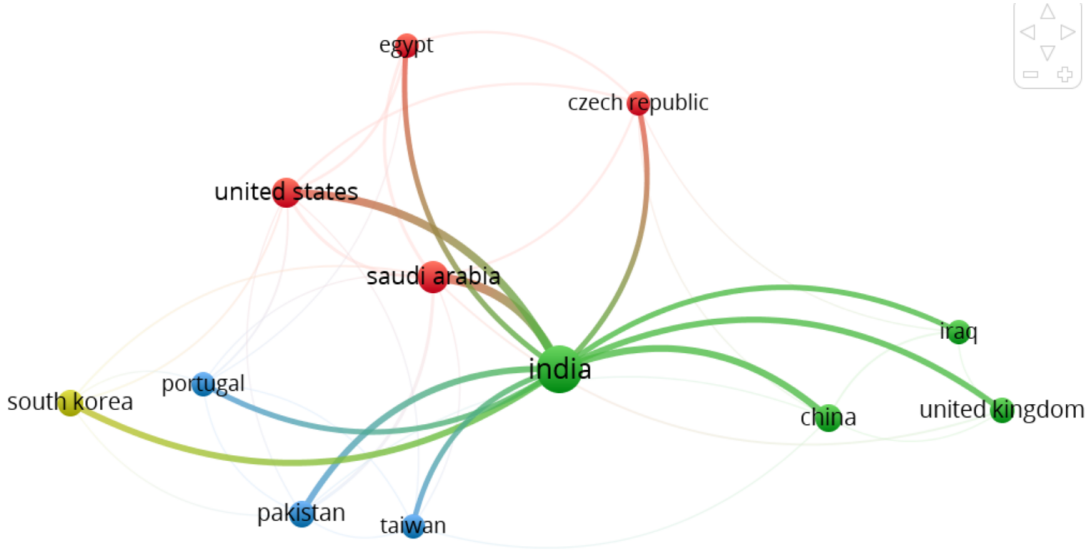


Figure 5 (b). Country co-authorship network

Geographical analysis and collaboration analysis illustrate that the research on blockchain for IoMT has been carried out in various countries, and scientific collaboration has been growing among various countries. Additionally, the co-authorship network signifies that leading contributing countries are linked to each other by joint exploration ties, highlighting the international interest in a safe and decentralized healthcare environment, as shown in Figure 5 (b). Together, the progressive, geographical, and collaboration patterns offer a view of the evolution and scientific context of blockchain-enabled IoMT research, thus answering RQ1. The geographical and collaboration analysis overall gives insight into the overall development and collaborative structure of the domain.

Table 4. Country-wise citation per year

Country	Total citations	Average Citations
India	948	10.3
Korea	298	99.3
Hong Kong	164	82
Canada	160	80
Malaysia	126	63
Saudi Arabia	114	22.8
China	107	35.7
Ethiopia	89	89
Finland	85	85
United Arab Emirates	73	36.5

An additional perspective on the regional impact of blockchain-enabled IoMT research is offered by the citation analysis. India has the most citations overall (948), demonstrating its significant contribution to the field of knowledge as shown in Table 4. The average citation impact, however, varies significantly between countries.

The average number of citations per article is highest in K orea (99.3), followed by Ethiopia (89), Finland (85), Hong Kong (82), and Canada (80). These results show that publication productivity and citation impact do not always follow the same pattern, as highly cited contributions can still have a significant academic effect in nations with fewer publications. Overall, the geographic and collaborative analyzes show that the worldwide research environment in blockchain-enabled IoMT is inconsistent but becoming more integrated. The co-authorship network emphasizes the increasing significance of worldwide scientific cooperation, and the top contributing nations show significant research effort. Together, these results partially answer RQ2 by offering proof of geographic contribution, collaborative structure, and research influence.

5.3 Keyword Analysis and Conceptual Structure of Blockchain-Enabled System

A conceptual structure of blockchain-based IoMT studies was explored by conducting a keyword co-occurrence analysis to detect the key research themes and relationships between the most frequently studied concepts. Thematic analysis of a research field can be obtained from the keyword co-occurrence analysis, which investigates the co-occurrence of different concepts in the scientific literature. The resulting network has larger nodes for more often occurring keywords, links as relationships between keywords, and clusters as groups of closely related research concepts.

According to the analysis, blockchain, Internet of Medical Things, Internet of Things (IoT), healthcare, security, and privacy are some of the significant concepts in the research arena. They are grouped in the center, suggesting that the research work already done has mainly been based on the application of blockchain to enhance trust, security, privacy, and the management of healthcare data in a connected healthcare environment.

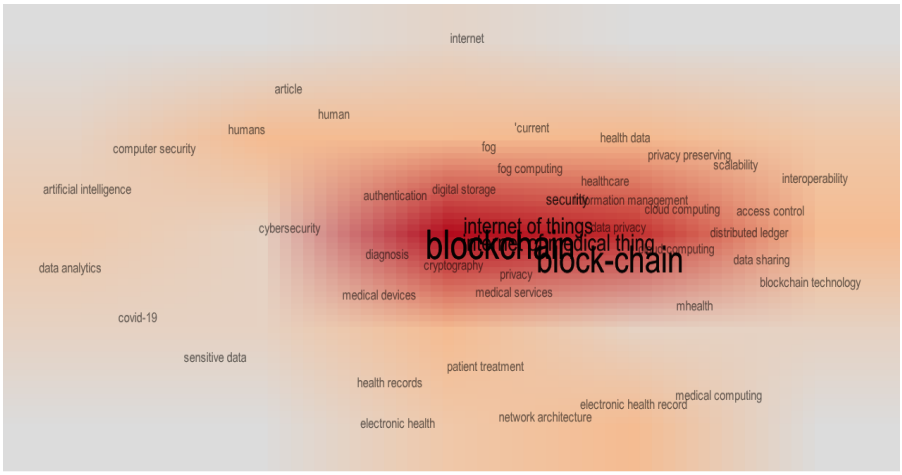


Figure 5 (c). Keyword co-occurrence network

Security and privacy play an important role in the conceptual framework of blockchain-based IoMT research. This indicates that the relationship between blockchain and healthcare, as well as IoMT, has considerable attention in the literature, as shown in Figure 5(c), particularly in securing sensitive healthcare information, ensuring data integrity, and enhancing authentication. The increasing interest in automated and decentralized approaches to the management of authorization and secure data exchange is also reflected in the concepts of smart contracts.

The intimate relationship between blockchain, IoMT, healthcare, and data-related ideas indicates that blockchain is being studied more and more for decentralized and traceable healthcare-data sharing in addition to security.

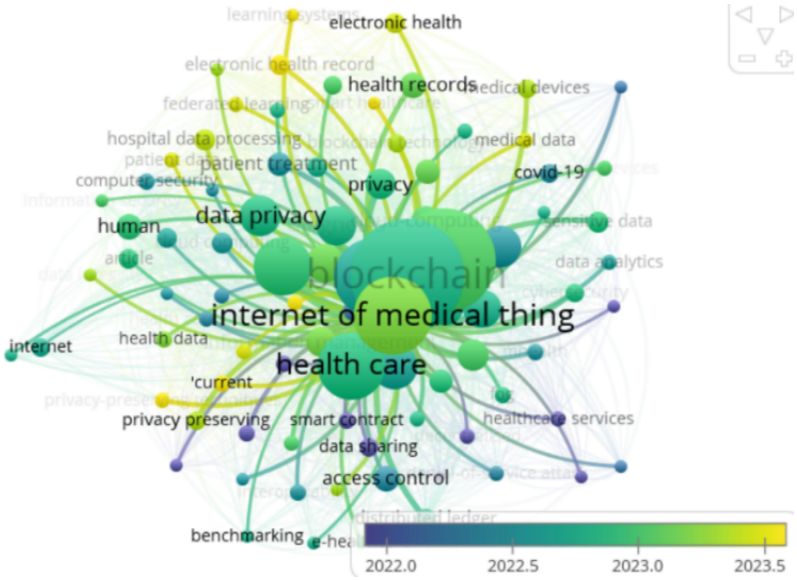


Figure 5 (d). Co-occurrence with index keyword

The co-occurrence relationships among the index keywords of selected publications are shown in Figure 5(d). The main concepts that are influencing the research domain are shown in the prominent nodes, which include blockchain, Internet of Medical Things, IoT, healthcare, security, and privacy. The relationships between these keywords also illustrate how security, healthcare data management, and blockchain in IoMT applications are tightly coupled domains of research.

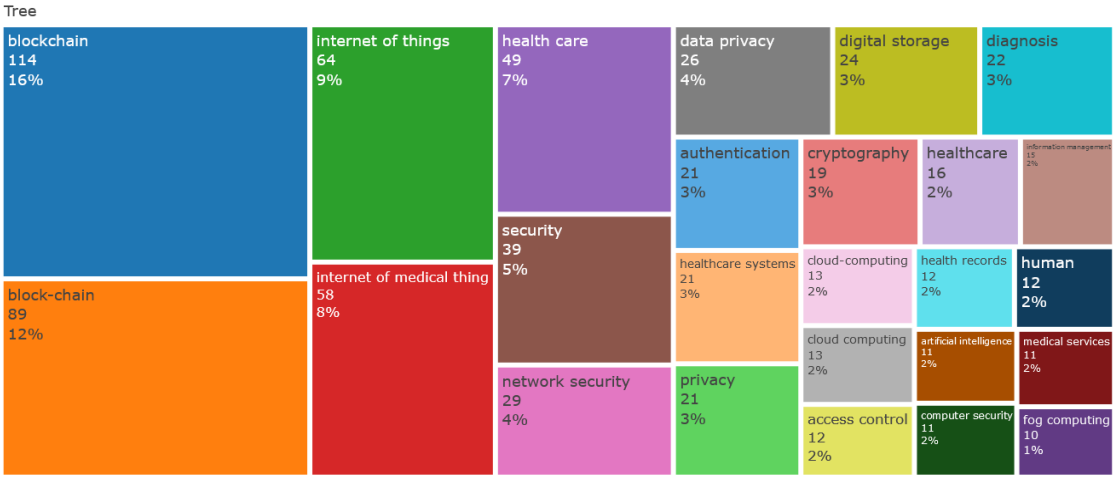


Figure 5(e). Tree diagram with different keywords

The tree diagram in Figure 5(e) is a complementary visualization of the main keywords that were found in the dataset. The relative significance of the terms indicates the key research interests and gives a hierarchical overview of the conceptual composition of blockchain-based IoMT research.

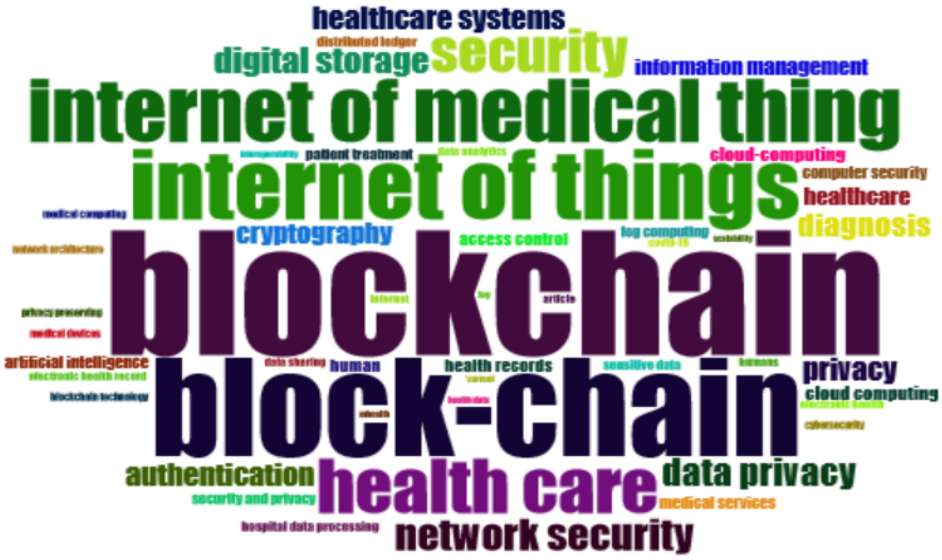


Figure 5 (f). Word state

Figure 5(f) further summarizes the frequency of important research terms by a word-cloud representation. The keyword co-occurrence analysis further highlights the importance of these keywords and their central role in the analyzed literature, with the word "blockchain" appearing prominently alongside other keywords such as IoMT, healthcare, security, privacy, etc.

In addition to the network-based representation, Table 5 shows the most common keywords found in the bibliometric data. The frequency of keywords also gives insights into the concepts that are the subject of continuous research and study in the area of blockchain-based IoMT.

Table 5. Frequently used words in bibliometric analysis

Words	Occurrences
blockchain	114
block-chain	89
Internet of Things (IoT)	64

Internet of medical things (IoMT)	58
health care	49
security	39
network security	29
data privacy	26
digital storage	24
diagnosis	22

The frequency distribution confirms the patterns in the co-occurrence network. The research field is mainly characterised by the use of blockchain and IoMT-related terms, followed by healthcare, security, network security, data privacy, digital storage and diagnosis. The high frequency of security & privacy highlights the importance of securing healthcare information, while the use of digital storage and digital diagnosis indicates the advancements of blockchain-IoMT research in the context of healthcare data management or application-centric medical environments.

Overall, from the combination of the keyword-based analyses, it can be seen that the conceptual structure of blockchain-based IoMT research is mainly focused on blockchain, healthcare, IoMT, security, privacy, and data-management-related concepts. These research domains are interconnected to show that the field is moving towards secure and distributed Healthcare Environments.

5.4 Role of Blockchain in Addressing IoMT Requirements

The bibliometric results show that blockchain is mainly explored in IoMT applications to address security, privacy, data integrity, access control, and sharing of data needs. Its decentralized and tamper-proof nature allows for the secure and decentralized recording and verification of healthcare transactions, eliminating the need for a central authority [21]. Smart contracts also facilitate automated access and control of potentially sensitive patient data, and blockchain identity systems enhance accountability among stakeholders. Existing studies then suggest that blockchain can be used as a tool to ensure trust and integrity in the protection of healthcare information in distributed IoMT settings. The results of this research indicate that blockchain is transitioning from securing transactions to a larger platform for trusted healthcare data management and exchange [28]. Its practical effectiveness, however, is limited by the need to solve the following issues: scalability, interoperability, computational overhead, and real-time processing needs [35].

Table 6. IoMT requirements to blockchain-enabled mechanisms and their contributions

IoMT Requirement	Role of Blockchain	Expected contribution
Security	Decentralized and tamper-resistant transactions	Protects healthcare information from unauthorized access
Privacy	Controlled and verifiable data	Protection of sensitive patient information
Data integrity	Immutable transaction history	Enables verification of data authenticity
Secure data sharing	Distributed and auditable data exchange	Interaction among healthcare participants
Traceability	Timestamped and verifiable records	Improves accountability of healthcare-data operations
Identity management	Blockchain-supported authentication records	Trust among participating devices and stakeholders

The results show that, overall, blockchain is mainly used for establishing trust and ensuring the security of sensitive healthcare information, access-control policies and data integrity, as well as secure and traceable data exchange in IoMT research. Overall, the findings determine that blockchain contributes to security, data integrity, access control, privacy, and trusted healthcare-data exchange in IoMT environments, which addresses RQ3.

5.5 Challenges in blockchain-based IoMT system

While the adoption of blockchain has the potential to enhance the security, privacy, integrity, and trust of medical IoT, there are several technical and operational barriers to its widespread use in healthcare. Scalability, interoperability, computational and energy overhead, latency, and real-time processing are the primary technological concerns identified in the reviewed literature. In IoMT, medical devices continuously produce vital data with varying formats and timeliness, which poses a special challenge in terms of these limitations. The regulatory and compliance requirements add to the challenges of implementing and sharing sensitive medical data across organizations.

Table 7. Key challenges, potential solutions, and future research directions for blockchain-enabled IoMT

Challenge	Impact on IoMT	Future research direction
Scalability	Increasing transactions from large numbers of medical devices	Lightweight and scalable consensus mechanisms
Interoperability	Difficulty in exchanging data among heterogeneous IoMT platforms	Standardized and interoperable architectures
Computational and energy overhead	Resource-constrained IoMT devices cannot support intensive blockchain operations	Lightweight cryptography and energy-efficient blockchain
Latency and real-time processing	Consensus and transaction validation may delay time-sensitive healthcare operations	Edge/fog-assisted and hybrid blockchain architectures
Real-time decision support	Delayed processing can affect rapid clinical decision-making	Integration with AI and edge analytics

Scalability and real-time processing are two of these difficulties, especially considering the potential for the number of transactions and processing power needed on the blockchain to grow significantly as IoMT data grows, as shown in Table 7. For future research, lightweight consensus mechanisms and architectures for edge-assisted blockchain that can lower the processing burden and latency are needed. The issue of interoperability also needs to be given more attention to achieve seamless communication between the heterogeneous medical devices and healthcare platforms. Additionally, combining blockchain with AI and edge analytics could enable greater speed to decision-making and the security and transparency of healthcare data.

These findings indicate that scalability, computational efficiency, real-time processing, and regulatory compliance remain critical barriers to blockchain–IoMT deployment. Addressing these limitations represents an important direction for future research, which covers RQ4.

6. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

In this study, the evolution of Internet of Medical Things research in the field of blockchain technologies is analysed, focusing on the contributions of the different countries, the scientific cooperation among the different institutions, the main research trends, and the technological advances. The results show that researchers are increasingly interested in blockchain–IoMT integration and identify security, privacy, healthcare data management, and network security as key research directions. The geographical and collaboration analyses also show that an international research scene is developing.

The results show that blockchain is mainly explored to provide security, privacy, data integrity, access control, authentication, and trusted healthcare-data sharing in IoMT scenarios. But scalability requirements, latency, real-time processing, and regulations remain barriers to its real-world implementation. For resource-limited IoMT deployments, which produce continual, heterogeneous healthcare information, these challenges are especially critical. It is recommended that future research should be directed towards lightweight and scalable blockchain architectures, energy-efficient consensus mechanisms, edge-assisted processing, interoperability standards, and privacy-preserving mechanisms. The future of blockchain in IoMT could see adoption of new technologies like artificial intelligence, federated learning, and decentralized storage, further improving efficiency and scalability. Solving these technical and regulatory hurdles will be crucial in moving blockchain–IoMT solutions from their experimental phase to a practical and secure smart healthcare system. The limitations of the present study include Scopus as a database used, the search method used, and the study period. To capture the dynamic nature of the blockchain-IoMT research landscape, future bibliometric studies could take into account multiple scientific databases and the latest data sets.

REFERENCES

[1] Q Niu, H Li, Y Liu, et al., “Toward the Internet of Medical Things: Architecture, trends and challenges,” *Math Biosci Eng*, vol. 21, no. 1, pp. 650–678, 2024, doi: 10.3934/mbe.2024028.

[2] H. Verma, N. Chauhan, and L. K. Awasthi, “A Comprehensive review of ‘Internet of Healthcare Things’: Networking aspects, technologies, services, applications, challenges, and security concerns,” *Comput. Sci. Rev.*, vol. 50, pp. 591–609, 2023, doi: 10.1016/j.cosrev.2023.100591.

[3] R. U. Rasool, H. F. Ahmad, W. Rafique, et al., “Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML,” *J. Netw. Comput. Appl.*, vol. 201, no. 5, pp. 332–351, 2022, doi: https://doi.org/10.1016/j.jnca.2022.103332.

[4] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Cryptogr. Mail. List https//metzdowd.com*, 2008, [Online]. Available: http://www.bitcoin.org/bitcoin.pdf.

[5] R. Dwivedi, D. Mehrotra, and S. Chandra, “Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review,” *J. Oral Biol. Craniofacial Res.*, vol. 12, no. 2, pp. 302–318, 2022.

[6] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund,

"Blockchain technology in healthcare: a systematic review," in *Healthcare*, 2019, p. 56.

[7] P. Durneva, K. Cousins, and M. Chen, "The current state of research, challenges, and future research directions of blockchain technology in patient care: Systematic review," *J. Med. Internet Res.*, vol. 22, no. 7, pp. 619–636, 2020, doi: 10.2196/18619.

[8] M. Sookhak, M. R. Jabbarpour, N. S. Safa, et al., "Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues," *J. Netw. Comput. Appl.*, vol. 178, no. 5, pp. 950–979, 2021, doi: https://doi.org/10.1016/j.jnca.2020.102950.

[9] B. Zaabar, O. Cheikhrouhou, F. Jamil, et al., "HealthBlock: A secure blockchain-based healthcare data management system," *Comput. Networks*, vol. 200, p. 108500, 2021, doi: https://doi.org/10.1016/j.comnet.2021.108500.

[10] A. Sharma, R. K. Kaushal, and N. Kumar, "A Comprehensive Assessment of Blockchain Technology in the Healthcare Industry and Techniques to Store Medical Image," in *2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT)*, IEEE, 2024, pp. 1–7. doi: 10.1109/ICEEICT61591.2024.10718467.

[11] H. Taherdoost, "Blockchain-based internet of medical things," *Appl. Sci.*, vol. 13, no. 3, pp. 287–306, 2023, doi: https://doi.org/10.3390/app13031287.

[12] M. Garriga, S. Dalla Palma, M. Arias, et al., "Blockchain and cryptocurrencies: A classification and comparison of architecture drivers," *Concurr. Comput. Pract. Exp.*, vol. 33, no. 8, pp. 1–21, 2021, doi: 10.1002/cpe.5992.

[13] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, vol. 50, 2020, doi: 10.1016/j.jisa.2019.102407.

[14] S. Zeba, P. Suman, and K. Tyagi, "Types of blockchain," in *Distributed Computing to Blockchain*, Elsevier, 2023, pp. 55–68. doi: https://doi.org/10.1016/B978-0-323-96146-2.00003-6.

[15] A. Samadhiya, A. Kumar, J. A. Garza-Reyes, et al., "Unlock the potential: unveiling the untapped possibilities of blockchain technology in revolutionizing Internet of Medical Things-based environments through systematic review and future research propositions," *Inf. Sci. (Ny).*, vol. 661, pp. 140–177, 2024, doi: https://doi.org/10.1016/j.ins.2024.120140.

[16] A. Sharma, R. K. Kaushal, and N. Kumar, "Demystifying Blockchain Technology in Healthcare Perspective and its Implementation," in *2025 12th International Conference on Reliability, Infocom Technologies and Optimization(ICRITO)*, 2025, pp. 1–6. doi: 10.1109/ICRITO66076.2025.11241397.

[17] A. Alsadhan, A. Alhogail, and H. Alsalamah, "Blockchain-based privacy preservation for the internet of medical things: a literature review," *Electronics*, vol. 13, no. 19, pp. 832–852, 2024, doi: https://doi.org/10.3390/electronics13193832.

[18] K. Chafik, A. Ouaguid, M. Hanine, et al., "Exploring the intersection of blockchain and e-health: A bibliometric analysis of recent research," *Blockchain Res. Appl.*, vol. 22, pp. 431–482, 2025, doi: https://doi.org/10.1016/j.bcra.2025.100431.

[19] H. Xin, S.-S. M. Ajibade, G. N. Alhassan, et al., "Emerging trends and bibliometric analysis of internet of medical things for innovative healthcare (2016–2023)," *Digit. Heal.*, vol. 12, pp. 701–720, 2025, doi: 10.1177/20552076251395701.

[20] J. Miao, Z. Wang, Z. Wu, X. Ning et al., "A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things," *Expert Syst. Appl.*, vol. 237, pp. 329–346, 2024, doi: 10.1016/j.eswa.2023.121329.

[21] Y. Y. Ghadi *et al.*, "The role of blockchain to secure internet of medical things," *Sci. Rep.*, vol. 14, no. 1, pp. 422–453, 2024, doi: https://doi.org/10.1038/s41598-024-68529-x.

[22] L. Chen, T. Feng, R. Ma, et al., "BTMDS: Blockchain trusted medical data sharing scheme with privacy protection and access control," *Comput. Commun.*, vol. 225, pp. 279–288, 2024, doi: 10.1016/j.comcom.2024.07.007.

[23] K. Sabiri, F. Sousa, and T. Rocha, "A systematic review of privacy-preserving blockchain applications in healthcare," *Multimed. Tools Appl.*, vol. 84, no. 32, pp. 925–980, 2025, doi: https://doi.org/10.1007/s11042-024-20541-z.

[24] M. Aria and C. Cuccurullo, "bibliometrix: An R-tool for comprehensive science mapping analysis," *J. Informetr.*, vol. 11, no. 4, pp. 959–975, 2017, doi: https://doi.org/10.1016/j.joi.2017.08.007.

[25] W. Moulahi, I. Jdey, T. Moulahi, et al., "A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data," *Comput. Biol. Med.*, vol. 167, pp. 630–643, 2023, doi: https://doi.org/10.1016/j.compbiomed.2023.107630.

[26] G. Ganapathy, S. J. Anand, M. Jayaprakash, et al., "A blockchain-based federated deep learning model for secured data transmission in healthcare IoT networks," *Meas. Sensors*, vol. 33, pp. 176–185,

2024, doi: https://doi.org/10.1016/j.measen.2024.101176.

[27] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *J. Parallel Distrib. Comput.*, vol. 164, no. 6, pp. 152–167, 2022, doi: 10.1016/j.jpdc.2022.03.009.

[28] K. Fiaz *et al.*, "A two-phase blockchain-enabled framework for securing internet of medical things systems," *Internet of Things*, vol. 28, pp. 335–362, 2024, doi: https://doi.org/10.1016/j.iot.2024.101335.

[29] Q. Lin, X. Li, K. Cai, M. Prakash et al., "Secure Internet of Medical Things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking," *Inf. Sci. (Ny).*, vol. 654, pp. 783–796, 2024, doi: https://doi.org/10.1016/j.ins.2023.119783.

[30] O. Popoola, M. Rodrigues, J. Marchang, et al., "A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, challenges and solutions," *Blockchain Res. Appl.*, vol. 5, no. 2, pp. 178–228, 2024, doi: https://doi.org/10.1016/j.bcra.2023.100178.

[31] A. Rejeb, H. Treiblmaier, K. Rejeb, et al., "Blockchain research in healthcare: a bibliometric review and current research trends," *J. Data, Inf. Manag.*, vol. 3, pp. 109–124, 2021, doi: https://doi.org/10.1007/s42488-021-00046-2.

[32] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *bmj*, vol. 372, no. 4, pp. 1–10, 2021, doi: https://doi.org/10.1136/bmj.n71.

[33] N. J. Van Eck and L. Waltman, "Software survey: VOSviewer, a computer program for bibliometric mapping," *Scientometrics*, vol. 84, no. 2, pp. 523–538, 2010, doi: 10.1007/s11192-009-0146-3.

[34] N. Donthu, S. Kumar, D. Mukherjee, et al., "How to conduct a bibliometric analysis: An overview and guidelines," *J. Bus. Res.*, vol. 133, pp. 285–296, 2021, doi: https://doi.org/10.1016/j.jbusres.2021.04.070.

[35] S. Sutradhar, S. Majumder, R. Bose, et al., "A blockchain privacy-conserving framework for secure medical data transmission in the internet of medical things," *Decis. Anal. J.*, vol. 10, pp. 419–431, 2024, doi: https://doi.org/10.1016/j.dajour.2024.100419.