

Applications of Blockchain-Based Technology for Healthcare Devices Post-market Surveillance

Review began 03/28/2024
Review ended 04/06/2024
Published 04/08/2024

© Copyright 2024
Muniappan et al. This is an open access article distributed under the terms of the Creative Commons Attribution License CC-BY 4.0., which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Swarna Muniappan¹, Madhan Jeyaraman^{2, 3, 4}, Sankalp Yadav⁵, Naveen Jeyaraman⁵, Sathish Muthu^{6, 4, 7}, Swaminathan Ramasubramanian⁸, Bishnu P. Patro⁹

1. Electronics and Communication Engineering, Dr MGR Educational and Research Institute, Chennai, IND 2. Clinical Research, Virginia Tech India, Dr MGR Educational and Research Institute, Chennai, IND 3. Orthopaedics, ACS Medical College and Hospital, Dr MGR Educational and Research Institute, Chennai, IND 4. Department of Orthopaedics, Orthopaedic Research Group, Coimbatore, IND 5. Medicine, Shri Madan Lal Khurana Chest Clinic, New Delhi, IND 6. Department of Orthopaedics, Government Karur Medical College, Karur, IND 7. Department of Biotechnology, Faculty of Engineering, Karpagam Academy of Higher Education, Coimbatore, IND 8. Orthopaedics, Government Medical College, Omandurar Government Estate, Chennai, IND 9. Orthopaedics, All India Institute of Medical Sciences, Bhubaneswar, IND

Corresponding author: Sankalp Yadav, drsankalpyadav@gmail.com

Abstract

The volume of data analysis for medical device post-market surveillance (PMS) has increased dramatically in recent years. It is the more stringent and intricate regulatory criteria of the health authorities that are meant to improve the medical device safety review. As regulators scrutinize device safety more closely, proactive approaches to PMS processes are becoming crucial. To solve some of the issues brought on by this shifting regulatory landscape, new technologies have been investigated. This study envisages the technical features of blockchain technology (BCT) and its role in enhancing the PMS for medical devices. To address the aforementioned challenges, our model involves the establishment of a secure, permissioned blockchain for PMS data management, utilizing a proof-of-authority consensus mechanism. This blockchain framework will exclusively permit a carefully vetted and designated set of participants to validate transactions and record them in the PMS data ledger. The utilization of BCT holds the potential to introduce enhanced efficiency and provide several advantages to the various stakeholders involved in the PMS procedure, including its potential to support emerging regulatory efforts.

Categories: Epidemiology/Public Health, Medical Physics, Quality Improvement

Keywords: artificial intelligence, internet of things, medical device, block chain technology, post-marketing surveillance, blockchain

Introduction

The system for monitoring medical devices after they're released into the market, known as post-market surveillance (PMS), has been facing an exponential increase in data volume in recent times. This surge in data is largely due to the tightened regulatory standards set by health authorities, aimed at improving the safety assessments of medical devices [1,2]. These authorities are moving towards establishing a system where safety information is exchanged swiftly, reliably, and efficiently. The ultimate goal is to ensure that any safety risks associated with medical devices are detected promptly and that necessary corrective actions are taken without delay [3,4]. As a result of the increasing rigor in safety checks, there's a significant shift towards enhancing PMS systems to be more proactive. Industry stakeholders, including those responsible for ensuring the safety of medical devices, are fully aware of the challenges posed by the evolving regulatory environment. They acknowledge the urgent need to overcome these challenges and to close the existing gaps in the PMS processes [5].

Parallel to developments in other sectors of the medical device industry, there's a growing interest in the application of artificial intelligence (AI) technologies to revolutionize traditional, reactive PMS systems [6,7]. Among the array of technologies being explored, blockchain technology (BCT) has garnered significant attention over the past two years. Blockchain can essentially be described as a distributed ledger or database that facilitates data processing through a network of interconnected nodes [8]. Unlike conventional data-sharing methods that rely on a central authority for data management, blockchain offers a decentralized approach. This decentralization enables direct interactions among users, eliminating the need for third-party intermediaries. Traditionally, transactions between two parties (users A and B) required verification by a third party (user C), which could be a government agency or a healthcare regulatory body. However, with the advent of blockchain, this intermediary's role becomes obsolete. BCT empowers users to encode and record diverse types of transactions in a secure, immutable, and distributed ledger [9]. This innovation paves the way for transactional models that bypass traditional intermediaries, offering new levels of efficiency and security. The regulatory landscape for PMS is complex, marked by a need for robust data integrity, transparency, and traceability, alongside the requirement for rapid response mechanisms to adverse events. Blockchain technology, characterized by its decentralized, transparent, and immutable ledger system, offers a transformative solution to these challenges.

How to cite this article

Muniappan S, Jeyaraman M, Yadav S, et al. (April 08, 2024) Applications of Blockchain-Based Technology for Healthcare Devices Post-market Surveillance. Cureus 16(4): e57881. DOI 10.7759/cureus.57881

In this article, we delve into the current challenges faced by the PMS system, highlighting the complexities of managing increased data volumes and regulatory demands. We explore how blockchain technology can be harnessed to enhance PMS, discussing the strategies for its implementation and examining the potential it holds for transforming safety surveillance of medical devices. Additionally, we address the limitations of BCT in the context of PMS, providing a balanced perspective on its applicability and impact. Through this discussion, we aim to offer insights into the future of medical device safety and the role of innovative technologies in shaping it.

Technical Report

Blockchain technology

This article aims to examine the various technical facets of BCT and its potential to bolster ongoing efforts to enhance the PMS system for medical devices. A blockchain is a distributed and decentralized digital ledger, often publicly accessible, designed to record transactions across multiple computers [9]. Its fundamental feature is ensuring that once a record is added, it cannot be altered retroactively without modifying all subsequent blocks in the chain. Blockchain is an open-source technology that facilitates secure communication for tracking previous actions related to decentralized patient records [10,11]. For instance, it enables the effective sharing of safety data while upholding the principles of integrity, privacy, and accessibility [11]. This innovative approach has the potential to make substantial volumes of anonymized PMS data from diverse sources accessible, including unsolicited reports, medical device registries, and unconventional data sources [12-14].

With BCT, several participants in a network can share a single ledger that they can all rely on to be accurate. Every new transaction or piece of data is added to a "block," which is made up of all the previous blocks' hashes, linking them all together to form a chain of blocks known as a blockchain [5]. By continuously chaining hash-based proof-of-work transactions together, the network timestamps them and creates a record that cannot be changed without repeating the proof-of-work. These transactions are recorded and can be used to support payments and currencies, as well as provide safety information. Every new transaction on this network must be verified by a node in order to guarantee its completeness. Every block added to a blockchain makes each transaction in that block more unchangeable since every node in the network verifies it. The blockchain process's workflow is depicted in Figure 1.

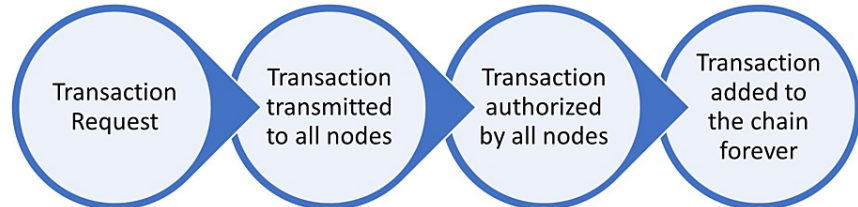


FIGURE 1: Illustration of process workflow in the blockchain technology

Picture courtesy: Dr. Sankalp Yadav and Swarna Muniappan

On a public blockchain, individuals have the capability to examine the ledger, and anyone can also contribute to and authenticate a block of transactions [9]. Conversely, in the context of private blockchains, it typically allows anyone on the internet to observe transaction blocks, but only designated individuals within organizations possess the authority to add and validate these blocks [10]. In the case of consortium blockchains, a specific category of groups within a company, such as banks, is granted the privilege to verify and add transactions, and the accessibility of the ledger can either be extended to a broader audience or confined to the chosen group [15-17].

Difficulties in providing sufficient PMS for medical equipment

It has been determined that the following problems will make it difficult to perform sufficient PMS on medical devices.

Security and Data Interchange

The rising integration of new technologies with medical equipment raises concern about potential PMS data

breaches, which must be prevented. It is essential to establish a secure environment for the swift and accurate sharing of data with authorized parties. One of the primary challenges in the safety signal detection process for medical devices is the timely exchange of PMS data between various sources and documents [7,18]. Recent public health crises have underscored the consequences of delayed identification of safety issues associated with promoted medical equipment.

Trackability of Medical Equipment

A robust PMS system necessitates the identification of the root cause behind adverse events. The examination of a sample of medical devices is essential for pinpointing the failure mode associated with an incident, but often this step falls short in determining the underlying cause [19,20].

Imitation

A recognized risk to patient safety is the counterfeiting of medical equipment. Increasing regulatory demands for further details regarding the provenance of medical devices have been made in an effort to solve this problem [21]. It is necessary to swiftly locate any medical device on the market in order to carry out safety-related regulatory measures, and this calls for the use of a Unique Device Identifier (UDI) [22].

Harmonization

The absence of uniformity and standardization among PMS data sources represents a significant challenge in the process of detecting safety signals for medical devices [18]. Each PMS data source contains unique content and employs different data storage methods. Two primary categories of medical device PMS data sources are spontaneous reporting systems and medical device registries, each with its own set of advantages and disadvantages.

Spontaneous Reporting Systems (SRS)

SRS are dynamic systems designed to capture patient injuries and product issues reported directly or through published articles [23]. Reports are sourced from patients, healthcare professionals, regulatory bodies, and manufacturers. The structure of SRS relies on establishing connections between events and specific medical devices. The extensive datasets collected are typically processed centrally, often within a database or repository, facilitating accessibility for analysis.

However, the absence of a globally harmonized standard dataset for reporting poses challenges in integrating data from diverse databases [24,25]. Moreover, a substantial portion of investigative findings remain inconclusive, and there is a bias towards reporting well-known adverse events or product issues related to medical devices, often influenced by social media or media coverage. Additionally, underreporting and over-reporting issues arise when medical devices undergo inadequate testing or inspection procedures [26].

Medical Device Registries

A medical device registry is a structured system with the primary objective of enhancing awareness of the role that medical devices play in elevating the quality of patient care consistently [27]. It systematically collects relevant data, evaluates significant outcomes, and comprehensively addresses the population's exposure to specific medical devices on a broad scale, ranging from global to national, regional, and healthcare system levels [28]. These registries typically contain essential information such as medical device details, diagnoses, prescriptions, medical histories, and procedures [29].

Unlike spontaneous reports, medical device registries are not limited to individuals who have experienced adverse effects or difficulties with medical devices [28]. Consequently, the data obtained from medical device registries offers distinct advantages that can complement more traditional PMS data sources, such as SRS. This includes the ability to conduct active PMS and confirmatory investigations. While the utilization of medical device registries offers numerous benefits, it is essential to acknowledge their associated limitations and drawbacks as well.

The registry's features may differ between nations due to variances in the consistency, granularity, and quality of the data, as well as in the length of the longitudinal follow-up, attrition rates, data privacy rules, legislation, and degree of information interchange [30,31]. A delay in the collection and consolidation of PMS data from foreign registries could result from the absence of standards among the various registries, which would ultimately delay the verification of safety signals. Device outcome data from the registry cannot be analyzed properly if a standardized UDI and nomenclature codes are not used. User errors are a major cause of unfavorable incidents involving medical equipment. To guarantee the safe handling of medical devices, it is imperative to develop suitable risk mitigation measures, primarily training.

BCT for PMS

Prospects for utilizing BCT to resolve issues with the PMS system in medical devices, either as a private permissioned blockchain or as a public permission-less blockchain, show promise. It might deal with a number of the issues that have been previously stated, as shown in Figure 2.

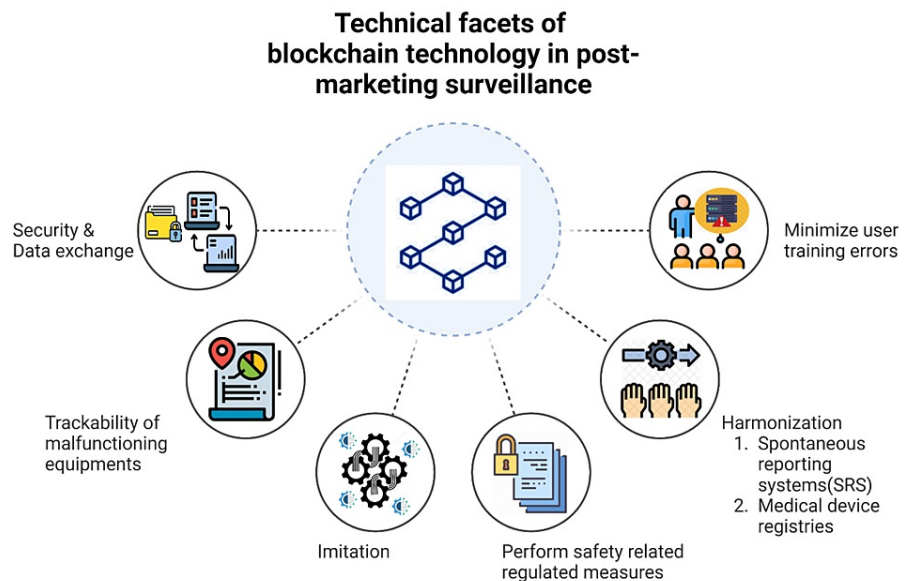


FIGURE 2: Technical facets of blockchain technology in improving the current limitations of traditional post-marketing surveillance

Picture courtesy: Dr. Madhan Jeyaraman and Dr. Sankalp Yadav

Trackability of Medical Equipment

The global adoption of UDI may very well be supported by BCT. Blockchain makes it possible to record production data as well as continuing use or maintenance data. Its unchangeable and dependable workflow will offer total traceability to medical device producers and proof of any safety concern related to that particular medical equipment. With the implementation of the European Union (EU) Medical Device Regulation's (MDR) extra traceability criteria, this kind of technology is becoming more and more important. According to the new rule, every product packaging must have a UDI that is readable by both computers and humans. Annex VI of the MDR addresses the utilization of data collection and automatic identification technologies, such as QR codes or bar codes, which have the potential for integration with BCT [7,32]. This integration envisions a scenario where a single bar code not only contains machine-readable data but also provides access to a blockchain traceability system.

Within this system, every stage of the supply chain and every interaction with the medical equipment is meticulously recorded by the blockchain traceability tool. Access to this blockchain would be extended to all economic operators involved with the medical equipment, allowing them to scrutinize the device's interactions comprehensively [7]. This approach facilitates efficient access to critical data for health authorities. Moreover, end-users can independently verify the authenticity of a medical device by scanning the blockchain, cross-referencing its data with the UDI database, and tracing its journey through the supply chain [33,34].

The regulation stipulates that "manufacturers must periodically verify the accuracy of all data relevant to the devices they have placed on the market" and implement "appropriate methods for validating the provided data" [35]. A blockchain-driven repository offers specific functionalities that align with the requirements of regulatory authorities.

Antitrust Actions and Fake Goods

The widespread implementation of UDI and BCT has the potential to significantly improve the efficiency of regulatory actions by enabling the comprehensive tracking of all medical products on the market and facilitating their swift and effective removal when necessary [36]. BCT possesses the capability to monitor

every stage of the medical equipment supply chain by meticulously tracking each transaction [37]. This integration of BCT can bolster data security, elevate the traceability of medical devices throughout the entire supply chain, and contribute to the detection and prevention of medical device fraud [38,39].

PMS Data Security, Standardization, and Interchange

Blockchain transactions are transparent, trustworthy, and secure records that cannot be duplicated or tampered with, making them valuable for detecting fraudulent activities [40]. BCT holds the potential to revolutionize the proactive approach to PMS data collection, encompassing spontaneous reports, registries, and nonstandard data sources [41]. It enables direct data acquisition without relying on the active reporting of adverse events. For instance, when a patient's information is registered in a medical device registry or a healthcare provider records a device-related adverse event in an electronic health record, this data can automatically become part of a shared block of information, eliminating the need for conscious incident reporting.

This innovative approach has the promise of significantly increasing the quantity of post-market data collected with minimal human intervention, ultimately enhancing the quality of the gathered PMS data [42]. Blockchain provides a decentralized and secure framework for sharing various types of safety information, making it less susceptible to cyberattacks [42]. New storage solutions that leverage BCT offer permanent and secure storage of medical device PMS data while maintaining efficiency and cost-effectiveness. The integration of blockchain in PMS has the potential to standardize data formats and content from various sources, enhance the security and efficiency of data exchange, ensure data integrity and transparency, and reduce the need for human intervention at each stage of data creation and retrieval [7,43]. The distributed nature of blockchain and the requirement for consensus to alter the chain enhance data integrity.

While public blockchains may lack privacy as data is open for inspection by all participants (albeit pseudonymized), "private" blockchains, restricted to select stakeholders, can provide the necessary privacy measures. These private blockchains can facilitate the exchange of PMS data among various stakeholders involved in the medical device safety evaluation process [44,45].

User Mistakes

BCT has the potential to expedite the identification of safety issues related to software devices caused by user error [46]. It can promptly inform the manufacturer about the nature of the fault and the specific training required for its resolution.

Strategic recommendations

A systematic implementation plan with clear goals, timelines, roles, and responsibilities is crucial for the successful integration of the private-permissioned blockchain into the PMS of medical devices. To fund this initiative, a consortium comprising various PMS stakeholders, including health authorities, manufacturers, and hospitals, should collectively provide financial support, with International Medical Device Regulatory Forum (IMDRF) assuming the role of coordinator [47]. Each member is required to pay annual fees to secure the necessary resources for implementing and operating the new PMS system for medical devices, built on the private, permissioned blockchain. This framework also has the potential for future expansion to include the Eudamed database.

Phase I: Standardization

IMDRF is a coalition of medical device regulators from different nations that have voluntarily joined together to harmonize regulatory requirements for medical products that vary across countries. This consortium includes regulatory bodies such as the Russian Ministry of Health, Singapore's HSA, Australia's TGA, Brazil's ANVISA, Health Canada, China FDA, the European Commission, Japanese PMDA and MHLW, and the US FDA [47-49]. IMDRF is embarking on an initiative to standardize PMS requirements across various jurisdictions. IMDRF will oversee the standardization efforts necessary for the implementation of the new system, ensuring that PMS data is consistently recorded in the blockchain system mentioned in the "Expert Review of Medical Devices" [47].

To reach a consensus on critical aspects like identifying PMS data sources, criteria for reporting adverse events, coding dictionaries for adverse events, and global device identification systems to be used in the new private permissioned blockchain, IMDRF will engage in negotiations with the diverse group of PMS stakeholders, which includes health authorities, hospitals, and manufacturers [7].

Phase II: Development of Permissioned Blockchain for Private Data and a New Global PMS Database

Once the global PMS requirements and the new global adverse event reporting dataset have been established, IMDRF will initiate collaboration with a technology partner to develop the software for the upcoming PMS global database. This software will be built upon a new private permissioned blockchain with

a proof-of-authority mechanism, ensuring the verification of every PMS data transaction [7]. To facilitate the use and participation in the new global PMS database, a governance framework will need to be created. All stakeholders, including health authorities, manufacturers, hospitals, and others, will need to reach a consensus and publicly disclose the regulations governing various aspects of the database. This includes rules related to accessibility, confidentiality, oversight, and regulatory reporting, as well as the agreements governing the permissioned blockchain for managing private data [50].

Phase III: Regional Pilot Program (US)

Following the consensus on global PMS standards, IMDRF will initiate a pilot program in the United States to implement the new private-permissioned blockchain system. In this endeavor, manufacturers will play a pivotal role in ensuring medical device traceability through blockchain by integrating BCT into their supply chain management processes [7]. Furthermore, they will be responsible for transitioning their existing PMS data sources, such as SRS and registries, to the blockchain platform.

As part of the pilot program, hospitals and health authorities participating in the initiative will need to commit to using blockchain for PMS data exchange. IMDRF will lead this pilot project, involving three US-based medical device companies, the FDA as a health authority, and three US hospitals. The primary objectives of this pilot are to demonstrate how blockchain can connect various systems and administrations to track a shared dataset containing patient data and product traceability information [7]. Additionally, it aims to showcase how BCT can potentially enhance the PMS of medical devices by expediting the process of notifying the supply chain about a medical device recall and facilitating the distribution of PMS data among stakeholders.

To facilitate the pilot, IMDRF will need to provide a technology partner and a consulting group. The technology partner will supply the PMS software, using the standardized reporting dataset established in Phase I, and will employ the blockchain infrastructure for verifying data transactions [7]. The consulting group will offer support, training, and oversight to pilot participants, ensuring accurate and comprehensive data recording throughout the process. Lessons learned from the pilot will be shared with all IMDRF members.

Phase IV: Global Pilot Program

Following the successful completion of the US pilot, a second pilot program will be launched on a global scale. IMDRF will once again play a crucial role in supporting this second pilot, which will involve nine medical device manufacturers (three from the US, three from the EU, and three from China), nine hospitals (three from the US, three from the EU, and three from China), and three health agencies (the FDA, European Commission, and China FDA) [51,52]. The primary objectives of this second pilot are to address unresolved issues and questions left by the US pilot and demonstrate how blockchain can connect various systems and administrations globally to track a shared dataset containing patient data and product traceability information while accommodating diverse local data privacy regulations. Additionally, it aims to illustrate how BCT could potentially enhance the PMS of medical devices on a global scale.

To facilitate the second pilot, IMDRF will need to provide a technology partner and a consulting group. These partners and consultants will collaborate with the manufacturers, hospitals, and national health authorities to supply the necessary tools, guidance, and support [51]. Given the global context, they will also play a crucial role in bridging any cultural gaps that may arise during the adoption of this new technology, such as language barriers, regional variations in technology, and the need to ensure PMS data confidentiality. The timeframe for the pilot is subject to adjustments and extensions. This flexibility will allow for modifications if any defects or limitations are identified during or after the pilot, or if additional areas of concern emerge to ensure the successful global adoption of the blockchain-based system. Lessons learned from the pilot will be shared with all IMDRF members.

Phase V: Global Blockchain Regulations

To ensure the successful implementation of the blockchain system by the globally agreed-upon GO-LIVE date, each local health authority will collaborate under the coordination of IMDRF [7]. They will develop and release local regulations and guidelines tailored to the specific needs of local hospitals and manufacturers. These regulations and guidelines will be established following the successful conclusion of the global pilot. The provided rules and guidelines will encompass instructions on how to manage data privacy, taking into account the pertinent local confidentiality laws. Additionally, the materials will outline the transition period for the worldwide implementation of the blockchain-based system, ensuring a smooth transition for all stakeholders involved.

Phase VI: Transitional Period

During the two-year transition period, PMS stakeholders will work in collaboration with the appropriate technology partner and consulting group (if required) to ensure a successful GO-LIVE date. The new private

PMS data-permissioned blockchain will replace existing systems like SRS and medical registries [7]. Within this two-year window, all hospitals, manufacturers, and health authorities will have the opportunity to migrate to the new blockchain system. To facilitate this transition, local health authorities will provide local PMS stakeholders with technology support and training, ensuring that they are well-prepared to deploy the new blockchain system by the predetermined deadline.

Phase VII: Global Launch

After the GO-LIVE date and the completion of the two-year transition period, a dedicated team within the IMDRF organization will monitor the usage of the new system for any potential issues [7]. This team will provide training and technology support as necessary. Local health authorities will play a key role in ensuring compliance with the new private PMS data-permissioned blockchain regulations. They will conduct regular inspections of the PMS systems of various local stakeholders to verify that they are effectively utilizing the technology and adhering to the established regulations.

Discussion

Limitations of BCT

In order to ensure the successful incorporation of BCT into the PMS process for medical devices, it is crucial to understand the challenges associated with this innovative technology.

Data Security and Privacy

BCT offers enhanced security by eliminating the need for third-party intermediaries in safety data transactions. However, it introduces certain privacy and security concerns due to its transparent nature, where the entire user community validates records within the blockchain architecture as opposed to a single external entity [5]. This lack of data privacy arises because every node can view the data transmitted by other nodes. In scenarios where a patient needs to designate a representative to access their information in emergencies, there is a risk that this representative may grant access to others, posing significant data privacy and security challenges. Another option to address these concerns is to implement robust security measures for the data, but this could impede data transfer across blocks and restrict access. Additionally, blockchain systems are vulnerable to a security breach known as a "51% attack," where a group of miners controlling over 50% of the nodes collaborates to manipulate the blockchain's contents [53]. This control allows them to halt new transactions, potentially disrupting the network, as evidenced by recent incidents affecting multiple coins. Furthermore, certain patient records may contain sensitive information that is unsuitable for inclusion on a blockchain, presenting additional complexities when using blockchain for PMS. To overcome these challenges, we propose the implementation of a private PMS data-permissioned blockchain with a proof-of-authority consensus mechanism [7,54-57]. This approach restricts the validation and addition of transactions to a small, vetted group of approved parties, addressing the aforementioned difficulties.

As an alternative, we may provide a trustworthy environment for decision-making, such as MedRec, a blockchain-based system that allows patients and medical practitioners to be authorized by manufacturers or health authorities to be new users of the private blockchain, safeguard, and recognize the PMS community members in charge of authorizing modifications and managing information sharing amongst the various parties involved [58,59]. Members of the PMS community now have the capability to contribute additional records associated with specific patients, and patients themselves can consent to sharing their records with other parties. All interactions among users and stakeholders prioritize utility, resulting in a single database where changes to patients' medical histories can be easily accessed. This concept holds the potential to enhance control over PMS data sharing for stakeholders and address data reliability issues, a prominent obstacle in PMS data exchange.

Another viable alternative involves ensuring complete data privacy for participants during PMS data transactions while maintaining transaction authenticity. However, in our private blockchain, some users may also be producers of medical equipment. In the conventional blockchain setup, participants could potentially access sensitive information about their competitors. To address this concern, our private PMS blockchain should implement a zero-knowledge proof algorithm method [60]. This method ensures that competitors cannot view transaction data belonging to their rivals while allowing transactions to be verified, thus eliminating the possibility of competitors gaining access to sensitive information about each other.

Oversee Data Retention

Effective management of data storage capacity poses a significant challenge. The traditional web and its associated data storage methods are vulnerable to data loss. In contrast, blockchain offers a decentralized data storage solution that is more resilient. BCT is primarily designed for tracking and executing data transactions. However, PMS generates substantial data volumes, necessitating frequent data archiving. Every node in the blockchain network must access the extensive PMS data stored in the blockchain, requiring substantial storage capacity [61]. The speed of identifying and editing events can be hindered by

the proliferation of PMS databases, which is problematic for situations where rapidity is crucial in PMS data transactions. To address this scalability issue, a blockchain solution should offer ample storage capacity while ensuring permanent retention of PMS data, all while maintaining fast performance and cost-effectiveness [62]. For instance, this solution could involve the development of a platform that allows users to store PMS data on a blockchain indefinitely without compromising speed or affordability.

Interoperability Issues

The design of PMS databases differs significantly from that of BCT, which is characterized by its distributed and decentralized nature. PMS databases are typically offline, centralized, and local in their structure. To effectively implement BCT in the context of PMS, a functional PMS database that can facilitate communication among various PMS stakeholders needs to be established [63]. One of the primary challenges in implementing BCT for PMS is that many international regulations still require central health authorities to govern PMS data exchanges with strict adherence to data privacy requirements. To address these challenges, a solution could involve the adoption of a private PMS-permissioned blockchain with a proof-of-authority consensus mechanism [50,64,65]. This approach would limit transaction validation and ledger updating to a small group of authorized and audited participants, including manufacturers, reporting facilities, and health authorities. To ensure the successful deployment of BCT, new international guidelines may need to be developed, and existing PMS data sources would need to transition to the new private PMS-permissioned blockchain system.

Standardization Issues

To enhance the standardization of secure PMS data sharing, the integration of BCT is a promising approach. However, it's important to note that BCT is still in its early stages, which may pose challenges when attempting to standardize its use in the context of medical device PMS. To address this, international health authorities should take the lead in establishing global standards for evaluating shared data concerning its volume, type, and structure in blockchain applications within the PMS domain [53,66,67]. In cases where there is a lack of harmonized data sets, individual nations or regions may create separate blocks with distinct data sets. It's crucial to emphasize that for blockchain applications to deliver value in PMS, several prerequisites must be met. This includes ensuring that existing PMS data exchange platforms are fully interconnected and compliant with all relevant business regulations, which should be automatically enforced to guarantee the effectiveness of blockchain implementations [68].

Behavioral Issues

In addition to the technical challenges previously discussed, BCT is still in its early stages, and it faces behavioral hurdles related to cultural shifts. While the medical device industry is gradually transitioning toward digitization, there is significant work ahead before traditional administrative PMS data exchange tools can be entirely replaced by BCT, which has yet to establish a proven track record in PMS data exchange [69,70]. Effectively transitioning medical professionals, patients, manufacturers, and health authorities away from paper records and toward technology will require patience and comprehensive training efforts. Currently, both the technology itself and the associated legal frameworks are met with skepticism due to their relatively low adoption rates in the healthcare sector as a whole. To address these challenges, stakeholders involved in the PMS process for medical devices should offer educational resources aimed at sharing the advantages and disadvantages of BCT in the medical device sector [71-73]. This proactive approach can help promote understanding and acceptance of blockchain within the industry.

Capital Investment

Collecting data on the blockchain and building the required number of blocks to ensure its immutability can be expensive due to a shortage of skilled professionals capable of developing blockchain infrastructure [43,66]. Consequently, there may be a need to accelerate transaction processing time, measured in the number of transactions per second, as PMS data exchanges require swift completion to ensure early detection of safety concerns. This might entail paying additional transactional fees, which can become costly depending on the accessibility of the network. It is essential to thoroughly evaluate the cost implications of integrating this new technology into the PMS system. Some hospitals still lack comprehensive computerization, which hinders their ability to exchange data with others, especially if they are not part of the same consortium. Achieving full blockchain-enabled IT systems will require a significant overhaul of existing IT infrastructure, potentially incurring high costs [3]. To address this financial burden, hospitals, manufacturers, and other PMS stakeholders should collectively contribute to support this technological advancement. Several entities have already initiated investigations into the application of BCT, with the European Commission launching the EU Blockchain Observatory and Forum [74]. This initiative aims to monitor PMS data, analyze trends, and address emerging concerns. Additionally, it is part of a broader effort to establish a blockchain standard for the European Union, with the potential for future extension to the Eudamed database [74].

Conclusions

BCT holds immense potential and offers significant synergy with the current needs of adopting PMS for medical devices. The successful implementation of our proposed solutions requires a solid understanding of the requirements and existing challenges within the medical device sector. It also necessitates continuous collaboration with a BCT specialist. The involvement of a BCT specialist is essential to ensuring that the new system operates effectively. Their expertise will eliminate the risk of the system failing due to developers lacking knowledge of how blockchain functions and its impact on the PMS process. This innovative approach has the potential to provide a more efficient means of managing medical device PMS, offering numerous benefits to the various stakeholders involved, including support for new regulatory initiatives.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Sankalp Yadav, Swarna Muniappan, Madhan Jeyaraman, Naveen Jeyaraman, Sathish Muthu, Swaminathan Ramasubramanian, Bishnu P. Patro

Acquisition, analysis, or interpretation of data: Sankalp Yadav, Swarna Muniappan, Madhan Jeyaraman, Naveen Jeyaraman, Sathish Muthu, Swaminathan Ramasubramanian, Bishnu P. Patro

Drafting of the manuscript: Sankalp Yadav, Swarna Muniappan, Madhan Jeyaraman, Naveen Jeyaraman, Sathish Muthu, Swaminathan Ramasubramanian, Bishnu P. Patro

Critical review of the manuscript for important intellectual content: Sankalp Yadav, Swarna Muniappan, Madhan Jeyaraman, Naveen Jeyaraman, Sathish Muthu, Swaminathan Ramasubramanian, Bishnu P. Patro

Supervision: Sankalp Yadav, Swarna Muniappan, Madhan Jeyaraman, Sathish Muthu, Swaminathan Ramasubramanian, Bishnu P. Patro

Disclosures

Human subjects: All authors have confirmed that this study did not involve human participants or tissue.

Animal subjects: All authors have confirmed that this study did not involve animal subjects or tissue.

Conflicts of interest: In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

Acknowledgements

Authors acknowledge the use of free language and grammar correction software like Grammarly for proof-reading of this manuscript.

References

1. Pane J, Francisca RD, Verhamme KM, Orozco M, Viroux H, Rebollo I, Sturkenboom MC: EU postmarket surveillance plans for medical devices. *Pharmacoepidemiol Drug Saf.* 2019, 28:1155-65. [10.1002/pds.4859](https://doi.org/10.1002/pds.4859)
2. Badnjević A, Pokvić LG, Deumić A, Bećirović LS: Post-market surveillance of medical devices: a review. *Technol Health Care.* 2022, 30:1315-29. [10.3233/THC-220284](https://doi.org/10.3233/THC-220284)
3. Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, Ishfaq M: Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future Internet.* 2022, 14:341. [10.3390/fi14110341](https://doi.org/10.3390/fi14110341)
4. Golosova J, Romanovs A: The advantages and disadvantages of the blockchain technology. 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE). Vilnius; 2018. 1-6. [10.1109/AIEEE.2018.8592253](https://doi.org/10.1109/AIEEE.2018.8592253)
5. Kearney B, McDermott O: The challenges for manufacturers of the increased clinical evaluation in the European medical device regulations: a quantitative study. *Ther Innov Regul Sci.* 2023, 57:783-96. [10.1007/s43441-023-00527-z](https://doi.org/10.1007/s43441-023-00527-z)
6. Gilbert S, Fenech M, Hirsch M, Upadhyay S, Biasucci A, Starlinger J: Algorithm change protocols in the regulation of adaptive machine learning-based medical devices. *J Med Internet Res.* 2021, 23:e30545. [10.2196/30545](https://doi.org/10.2196/30545)
7. Pane J, Verhamme KM, Shrum L, Rebollo I, Sturkenboom MC: Blockchain technology applications to postmarket surveillance of medical devices. *Expert Rev Med Devices.* 2020, 17:1123-32. [10.1080/17434440.2020.1825073](https://doi.org/10.1080/17434440.2020.1825073)
8. How does blockchain work?. (2023). Accessed: March 27, 2024: <https://online.stanford.edu/how-does-blockchain-work>.

9. Tyagi AK: Decentralized everything: practical use of blockchain technology in future applications . Distributed Computing to Blockchain. Pandey R, Goundar S, Fatima S (ed): Academic Press, Cambridge; 2023. 19-38. [10.1016/B978-0-323-96146-2.00010-3](https://doi.org/10.1016/B978-0-323-96146-2.00010-3)
10. Haleem A, Javaid M, Singh RP, Suman R, Rab S: Blockchain technology applications in healthcare: an overview. *Int J Intell Netw*. 2021, 2:150-9. [10.1016/j.ijin.2021.09.005](https://doi.org/10.1016/j.ijin.2021.09.005)
11. Fang HS, Tan TH, Tan YF, Tan CJ: Blockchain personal health records: systematic review . *J Med Internet Res*. 2021, 23:e25094. [10.2196/25094](https://doi.org/10.2196/25094)
12. Sun Z, Han D, Li D, Wang X, Chang CC, Wu Z: A blockchain-based secure storage scheme for medical information. *J Wireless Com Network*. 2022, 2022:40. [10.1186/s13638-022-02122-6](https://doi.org/10.1186/s13638-022-02122-6)
13. Kayikci S, Khoshgoftaar TM: Blockchain meets machine learning: a survey . *J Big Data*. 2024, 11:9. [10.1186/s40537-023-00852-y](https://doi.org/10.1186/s40537-023-00852-y)
14. Taherdoost H: Privacy and security of blockchain in healthcare: applications, challenges, and future perspectives. *Sci*. 2023, 5:41. [10.3390/sci5040041](https://doi.org/10.3390/sci5040041)
15. Allenbrand C: Smart contract-enabled consortium blockchains for the control of supply chain information distortion. *Blockchain Res Appl*. 2023, 4:100134. [10.1016/j.bcr.2023.100134](https://doi.org/10.1016/j.bcr.2023.100134)
16. Alam T: Blockchain-based internet of things: review, current trends, applications, and future challenges . *Computers*. 2023, 12:6. [10.3390/computers12010006](https://doi.org/10.3390/computers12010006)
17. Li S, Xu Q, Hou P, Chen X, Wang Y, Zhang H, Rong G: Exploring the challenges of developing and operating consortium blockchains: a case study. *EASE '20: Proceedings of the 24th International Conference on Evaluation and Assessment in Software Engineering*. Association for Computing Machinery, New York; 2020. 398-404. [10.1145/3385219.3385276](https://doi.org/10.1145/3385219.3385276)
18. Pane J, Verhamme KM, Villegas D, Gamez L, Rebollo I, Sturkenboom MC: Challenges associated with the safety signal detection process for medical devices. *Med Devices (Auckl)*. 2021, 14:43-57. [10.2147/MDER.S278868](https://doi.org/10.2147/MDER.S278868)
19. Amoores JN: A structured approach for investigating the causes of medical device adverse events . *J Med Eng*. 2014, 2014:514138. [10.1155/2014/514138](https://doi.org/10.1155/2014/514138)
20. Singh G, Patel RH, Boster J: Root cause analysis and medical error prevention. *StatPearls*. StatPearls Publishing, Treasure Island; 2024.
21. Marešová P, Klímová B, Honegr J, Kuča K, Ibrahim WN, Selamat A: Medical device development process, and associated risks and legislative aspects-systematic review. *Front Public Health*. 2020, 8:308. [10.3389/fpubh.2020.00308](https://doi.org/10.3389/fpubh.2020.00308)
22. Tcheng JE, Nguyen MV, Brann HW, et al.: The medical device unique device identifier as the single source of truth in healthcare enterprises - roadmap for implementation of the clinically integrated supply chain. *Med Devices (Auckl)*. 2021, 14:459-67. [10.2147/MDER.S344132](https://doi.org/10.2147/MDER.S344132)
23. Alomar M, Tawfiq AM, Hassan N, Palaian S: Post marketing surveillance of suspected adverse drug reactions through spontaneous reporting: current status, challenges and the future. *Ther Adv Drug Saf*. 2020, 11:2042098620958595. [10.1177/2042098620958595](https://doi.org/10.1177/2042098620958595)
24. Sivarajah U, Kamal MM, Irani Z, Weerakkody V: Critical analysis of big data challenges and analytical methods. *J Bus Res*. 2017, 70:263-86. [10.1016/j.jbusres.2016.08.001](https://doi.org/10.1016/j.jbusres.2016.08.001)
25. Martínez-García M, Hernández-Lemus E: Data integration challenges for machine learning in precision medicine. *Front Med (Lausanne)*. 2021, 8:784455. [10.3389/fmed.2021.784455](https://doi.org/10.3389/fmed.2021.784455)
26. Tase A, Ni MZ, Buckle PW, Hanna GB: Current status of medical device malfunction reporting: using end user experience to identify current problems. *BMJ Open Qual*. 2022, 11:10.1136/bmjopen-2022-001849
27. Li J, Mao Y, Zhang J: Maintenance and quality control of medical equipment based on information fusion technology. *Comput Intell Neurosci*. 2022, 2022:933328. [10.1155/2022/933328](https://doi.org/10.1155/2022/933328)
28. Registries for medical devices. *Registries for Evaluating Patient Outcomes: A User's Guide*. 3rd edition. Gliklich RE, Dreyer NA, Leavy MB (ed): Agency for Healthcare Research and Quality, Rockville; 2014. 13:EHC111.
29. Paul M, Maglaras L, Ferrag MA, Almmani I: Digitization of healthcare sector: a study on privacy and security concerns. *ICT Express*. 2023, 9:571-88. [10.1016/j.ict.2023.02.007](https://doi.org/10.1016/j.ict.2023.02.007)
30. Arts DG, De Keizer NF, Scheffer GJ: Defining and improving data quality in medical registries: a literature review, case study, and generic framework. *J Am Med Inform Assoc*. 2002, 9:600-11. [10.1197/jamia.m1087](https://doi.org/10.1197/jamia.m1087)
31. Melvin T, Torre M: New medical device regulations: the regulator's view. *EFORT Open Rev*. 2019, 4:351-6. [10.1302/2058-5241.4.180061](https://doi.org/10.1302/2058-5241.4.180061)
32. Annex VI - Information to be submitted upon the registration of devices and economic operators in accordance with articles 29(4) and 31, core data elements to be provided to the UDI database together with the UDI-DI in accordance with articles 28 and 29, and the UDI system. (2024). Accessed: March 27, 2024: <https://www.medical-device-regulation.eu/tag/annex-vi-information-to-be-submitted-upon-the-registration-of-devices-an...>
33. Khezr S, Moniruzzaman M, Yassine A, Benlamri R: Blockchain technology in healthcare: a comprehensive review and directions for future research. *Appl Sci*. 2019, 9:1736. [10.3390/app9091736](https://doi.org/10.3390/app9091736)
34. Nanda SK, Panda SK, Dash M: Medical supply chain integrated with blockchain and IoT to track the logistics of medical products. *Multimed Tools Appl*. 2023, 1-23. [10.1007/s11042-023-14846-8](https://doi.org/10.1007/s11042-023-14846-8)
35. Unique device identification system (udi system) . (2024). Accessed: March 27, 2024: <https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/unique-device-identification-sy...>
36. Wilson NA, Tcheng JE, Graham J, Drozda JP Jr: Advancing patient safety surrounding medical devices: a health system roadmap to implement unique device identification at the point of care. *Med Devices (Auckl)*. 2021, 14:411-21. [10.2147/MDER.S339232](https://doi.org/10.2147/MDER.S339232)
37. Taherdoost H: Blockchain and healthcare a critical analysis of progress and challenges in the last five years . *Blockchains*. 2023, 1:73-89. [10.3390/blockchains1020006](https://doi.org/10.3390/blockchains1020006)
38. Jadhav JS, Deshmukh J: A review study of the blockchain-based healthcare supply chain . *Soc Sci Humanit*. 2022, 6:100528. [10.1016/j.ssaho.2022.100528](https://doi.org/10.1016/j.ssaho.2022.100528)
39. Ahmed WA, MacCarthy BL: Blockchain-enabled supply chain traceability - how wide? how deep? . *Int J Prod*

- Econ. 2023, 263:108963. [10.1016/j.ijpe.2023.108963](https://doi.org/10.1016/j.ijpe.2023.108963)
40. Javaid M, Haleem A, Singh RP, Suman R, Khan S: A review of blockchain technology applications for financial services. *Tbench*. 2022, 2:100073. [10.1016/j.tbench.2022.100073](https://doi.org/10.1016/j.tbench.2022.100073)
 41. Cioeta R, Cossu A, Giovagnoni E, Rigoni M, Muti P: A new platform for post-marketing surveillance and real-world evidence data collection for substance-based medical devices. *Front Drug Saf Regul*. 2022, 2:10.3589/fdsfr.2022.992359
 42. Alajlan R, Alhumam N, Frikha M: Cybersecurity for blockchain-based iot systems: a review. *Appl Sci*. 2023, 13:7452. [10.3390/app13137452](https://doi.org/10.3390/app13137452)
 43. Tripathi G, Ahad MA, Casalino G: A comprehensive review of blockchain technology: underlying principles and historical background with future challenges. *Decis Anal*. 2023, 9:100544. [10.1016/j.dajour.2023.100344](https://doi.org/10.1016/j.dajour.2023.100344)
 44. Kiania K, Jameii SM, Rahmani AM: Blockchain-based privacy and security preserving in electronic health: a systematic review. *Multimed Tools Appl*. 2023, 1-27. [10.1007/s11042-023-14488-w](https://doi.org/10.1007/s11042-023-14488-w)
 45. Taherdoost H: The role of blockchain in medical data sharing. *Cryptography*. 2023, 7:36. [10.3390/cryptography7030036](https://doi.org/10.3390/cryptography7030036)
 46. Saeed H, Malik H, Bashir U, et al.: Blockchain technology in healthcare: a systematic review. *PLoS One*. 2022, 17:e0266462. [10.1371/journal.pone.0266462](https://doi.org/10.1371/journal.pone.0266462)
 47. International Medical Device Regulators Forum. (2024). Accessed: March 27, 2024: <https://www.imdrf.org/working-groups/imdrf-management-committee>.
 48. Wang C, Lee C, Shin H: Digital therapeutics from bench to bedside. *NPJ Digit Med*. 2023, 6:38. [10.1038/s41746-023-00777-z](https://doi.org/10.1038/s41746-023-00777-z)
 49. International Cooperation - European Commission. (2024). Accessed: March 27, 2024: https://health.ec.europa.eu/medical-devices-dialogue-between-interested-parties/international-cooperation_en.
 50. Zhou S, Li K, Xiao L, Cai J, Liang W, Castiglione A: A systematic review of consensus mechanisms in blockchain. *Mathematics*. 2023, 11:2248. [10.3390/math11102248](https://doi.org/10.3390/math11102248)
 51. About IMDRF. (2024). Accessed: March 27, 2024: <https://www.imdrf.org/about>.
 52. Awad S, Aljuburi L, Lumsden RS, Mpandzou M, Marinus R: Connected health in US, EU, and China: opportunities to accelerate regulation of connected health technologies to optimize their role in medicines development. *Front Med (Lausanne)*. 2023, 10:1248912. [10.3389/fmed.2023.1248912](https://doi.org/10.3389/fmed.2023.1248912)
 53. Shi S, He D, Li L, Kumar N, Khan MK, Choo KR: Applications of blockchain in ensuring the security and privacy of electronic health record systems: a survey. *Comput Secur*. 2020, 97:101966. [10.1016/j.cose.2020.101966](https://doi.org/10.1016/j.cose.2020.101966)
 54. Zhang P, Schmidt DC, White J, Dubey A: Consensus mechanisms and information security technologies. *Advances in Computers*. Kim S, Deka GC, Zhang P (ed): Elsevier, Amsterdam; 2019. 181-209. [10.1016/bs.adcom.2019.05.001](https://doi.org/10.1016/bs.adcom.2019.05.001)
 55. Kasi NR, S R, Karuppiyah M: Blockchain architecture, taxonomy, challenges, and applications. *Blockchain Technology for Emerging Applications*. Islam SH, Pal AK, Samanta D, Bhattacharyya S (ed): Academic Press, Cambridge; 2022. 1-31. [10.1016/B978-0-323-90193-2.00001-6](https://doi.org/10.1016/B978-0-323-90193-2.00001-6)
 56. Baranwal G, Kumar D, Vidyarthi DP: Blockchain based resource allocation in cloud and distributed edge computing: a survey. *Comput Commun*. 2023, 209:469-98. [10.1016/j.comcom.2023.07.023](https://doi.org/10.1016/j.comcom.2023.07.023)
 57. Islam MM, Merlec MM, In HP: A comparative analysis of proof-of-authority consensus algorithms: Aura vs Clique. *IEEE SSE*. 2022, 2022:327-32. [10.1109/SCCS55611.2022.00054](https://doi.org/10.1109/SCCS55611.2022.00054)
 58. Anik FI, Sakib N, Shahriar H, Xie Y, Nahiyah HA, Ahamed SI: Unraveling a blockchain-based framework towards patient empowerment: a scoping review envisioning future smart health technologies. *Smart Health (Amst)*. 2023, 29:100401. [10.1016/j.smhl.2023.100401](https://doi.org/10.1016/j.smhl.2023.100401)
 59. Khatoun A: A blockchain-based smart contract system for healthcare management. *Electronics*. 2020, 9:94. [10.3390/electronics9010094](https://doi.org/10.3390/electronics9010094)
 60. Pop CD, Antal M, Cioara T, Anghel I, Salomie I: Blockchain and demand response: zero-knowledge proofs for energy transactions privacy. *Sensors (Basel)*. 2020, 20:10.3390/s20195678
 61. Al Ahmed MT, Hashim F, Jahari Hashim S, Abdullah A: Hierarchical blockchain structure for node authentication in iot networks. *Egypt Inform J*. 2022, 23:545-61. [10.1016/j.eij.2022.02.005](https://doi.org/10.1016/j.eij.2022.02.005)
 62. Wang Y, Cong X, Zi L, Xiang Q: Blockchain for credibility in educational development: key technology, application potential, and performance evaluation. *Secur Commun Netw*. 2023, 2023:e5614241. [10.1155/2023/5614241](https://doi.org/10.1155/2023/5614241)
 63. Tiwari S, Sharma P, Choi TM, Lim A: Blockchain and third-party logistics for global supply chain operations: stakeholders' perspectives and decision roadmap. *Transp Res E Logist Transp Rev*. 2023, 170:103012. [10.1016/j.tre.2022.103012](https://doi.org/10.1016/j.tre.2022.103012)
 64. Hussein Z, Salama MA, El-Rahman SA: Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. *Cybersecurity*. 2023, 6:30. [10.1186/s42400-023-00163-y](https://doi.org/10.1186/s42400-023-00163-y)
 65. Singh A, Click K, Parizi RM, Zhang Q, Dehghantanha A, Choo KR: Sidechain technologies in blockchain networks: an examination and state-of-the-art review. *J Netw Comput Appl*. 2020, 149:102471. [10.1016/j.jnca.2019.102471](https://doi.org/10.1016/j.jnca.2019.102471)
 66. Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH: Blockchain application in healthcare systems: a review. *Systems*. 2023, 11:38. [10.3390/systems11010038](https://doi.org/10.3390/systems11010038)
 67. Abu-Elezz I, Hassan A, Nazeemudeen A, Househ M, Abd-Alrazaq A: The benefits and threats of blockchain technology in healthcare: a scoping review. *Int J Med Inform*. 2020, 142:104246. [10.1016/j.ijmedinf.2020.104246](https://doi.org/10.1016/j.ijmedinf.2020.104246)
 68. Casino F, Dasaklis TK, Patsakis C: A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telemat Inform*. 2019, 36:55-81. [10.1016/j.tele.2018.11.006](https://doi.org/10.1016/j.tele.2018.11.006)
 69. Digitalization in the medical device industry: analyzing innovation, investment and hiring trends. (2024). Accessed: March 27, 2024: <https://www.medicaldevice-network.com/data-insights/digitalization-in-medical/>.
 70. Digital transformation in the medical device industry: benefits and examples. (2024). Accessed: March 27, 2024: <https://kanerika.com/blogs/digital-transformation-in-the-medical-device->

industry/#:-:text=Examples%20include%20predic....

71. Woudstra K, Reuzel R, Rovers M, Tummers M: An overview of stakeholders, methods, topics, and challenges in participatory approaches used in the development of medical devices: a scoping review. *Int J Health Policy Manag.* 2023, 12:6839. [10.34172/ijhpm.2022.6839](https://doi.org/10.34172/ijhpm.2022.6839)
72. Regulatory overview on the importance of pms for medical devices in India . (2024). Accessed: March 27, 2024: <https://www.freysolutions.com/blog/the-importance-of-pms-for-medical-devices-in-india-a-regulatory-overview>.
73. Freitas L, Vieira AC, Oliveira MD, Monteiro H, Bana E Costa CA: Which value aspects are relevant for the evaluation of medical devices? Exploring stakeholders' views through a Web-Delphi process. *BMC Health Serv Res.* 2023, 23:593. [10.1186/s12913-023-09550-0](https://doi.org/10.1186/s12913-023-09550-0)
74. European commission launches the EU blockchain observatory and forum . (2024). Accessed: March 27, 2024: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_521.