Expert Review of Medical Devices

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ierd20

Blockchain technology applications to postmarket surveillance of medical devices

Josep Pane, Katia M.C. Verhamme, Lacey Shrum, Irene Rebollo & Miriam C.J.M. Sturkenboom

To cite this article: Josep Pane, Katia M.C. Verhamme, Lacey Shrum, Irene Rebollo & Miriam C.J.M. Sturkenboom (2020) Blockchain technology applications to postmarket surveillance of medical devices, Expert Review of Medical Devices, 17:10, 1123-1132, DOI: 10.1080/17434440.2020.1825073

To link to this article: https://doi.org/10.1080/17434440.2020.1825073

Published online: 03 Oct 2020.

EXPERT REVIEW OF MEDICAL DEVICES
2020, VOL. 17, NO. 10, 1123–1132
https://doi.org/10.1080/17434440.2020.1825073

Taylor & Francis
Taylor & Francis Group

ORIGINAL RESEARCH

OPEN ACCESS Check for updates

Blockchain technology applications to postmarket surveillance of medical devices

Josep Pane [a], Katia M.C. Verhamme [a], Lacey Shrum[b], Irene Rebollo[c] and Miriam C.J.M. Sturkenboom [d]

[a]Department of Medical Informatics, Erasmus Medical Center University of Rotterdam, Rotterdam, Netherlands; [b]3-Smart Kx, Vela Wood, Dallas, USA; [c]Department of CMO & Patient Safety, Novartis, Barcelona, Spain; [d]Department of Global Health, University Medical Center Utrecht, Netherlands

ABSTRACT

Introduction: The amount of mandatory data that needs to be analyzed as part of a medical device postmarket surveillance (PMS) system has grown exponentially in recent times. This is a consequence of increasingly demanding and complex regulatory requirements from Health Authorities, aimed at a better understanding of the medical device safety evaluation. Proactive approaches to PMS processes are becoming more necessary as regulators increase the scrutiny of device safety. New technologies have been explored to address some of the challenges associated with this changing regulatory environment.

Areas covered: This paper focuses on the different technical aspects of blockchain and how this new technology has the potential to support the ongoing efforts to improve the PMS system for medical devices.

Expert opinion: To address these challenges, we suggest to generate a private PMS data permissioned blockchain with a proof-of-authority consensus mechanism, to which only a restricted number of designated and audited participants have authorization to validate transactions and add them to the PMS data blockchain ledger. Blockchain has the potential to support a more efficient approach, which could offer many advantages to the different stakeholders involved in the PMS process, such as supporting with new regulatory initiatives.

ARTICLE HISTORY
Received 19 May 2020
Accepted 15 September 2020

KEYWORDS
Blockchain; medical devices; postmarket surveillance; safety evaluation; risk management

1. Introduction

The amount of required data that needs to be analyzed as part of a medical device postmarket surveillance (PMS) system has grown exponentially in recent times. This is a consequence of increasingly demanding and complex regulatory requirements from Health Authorities, aimed at a better understanding of the medical device safety evaluation. One of the main goals of the new regulations is to ensure a rapid, reliable and efficient exchange of PMS data to ensure medical device safety issues are identified in a timely manner, and appropriate action is taken accordingly. Proactive approaches to PMS processes are becoming more necessary as regulators increase the scrutiny of device safety [1,2]. This has led many of the stakeholders involved in the process of safety evaluation of medical devices to explore solutions to address some of the challenges associated with this changing regulatory environment. Furthermore, they understand the need to respond to some of the gaps associated with this process [3,4]. As in any other field of the medical device industry, the stakeholders have started working on artificial intelligence (AI) solutions that could help change the current reactive medical device PMS system. Some of the solutions that have been explored thus far in the area of medical devices include machine learning, robotic process automation, Internet of things and blockchain. Latter will be described briefly.

Blockchain technology has gained a high degree of attention over the past 2 years [5]. Blockchain can be understood as serving its users as a circulated database. That database permits its users to process data via specific nodes attached to the network. The traditional data exchange approach would have users maintain data via a centralized authority. Blockchain decentralizes that process and allows users to transact with one another without a third-party intervention, which is a major benefit of the blockchain process. As an example, let user C represent the so-called third party such as a governmental or healthcare regulatory body. Traditionally, if user A and user B wish to transact, user C would get involved to authenticate the identity of both users. However, in the blockchain setting, there is no more necessity for user C to intervene. The blockchain environment has led the way to new opportunities for transactions: a user may use blockchain technology to digitize, code and insert virtually any transaction of information in an immutable, distributed and secure manner.

In this paper, we will focus on the different technical aspects of blockchain and how this new technology has the potential to support the ongoing efforts to improve the PMS system for medical devices.

2. Blockchain technology

A blockchain is a decentralized, distributed, and oftentimes public, digital ledger that is used to record transactions

CONTACT Josep Pane jpanesalvado@gmail.com Depart. Of Medical Informatics, Erasmus MC – University of Rotterdam, Rotterdam 3000 CA, Netherlands

Article Highlights

- Proactive approaches topostmarket surveillance are becoming more necessary as regulators increase the scrutiny of medical device safety.
- Blockchain technology has the potential to solve some of the current challenges associated with the safety surveillance of medical devices by supporting device traceability, andefficient safety data exchange while maintaining data privacy, integrity and accessibility.
- Recommendations on how to address identified challenges related to the use of blockchain in the safety surveillance of medical devices are presented with a focus on solutions associated with data privacy, data storage, data exchange and data standardization.
- The suggested private postmarket surveillance data permissioned blockchain with a proof-of-authority consensus mechanism as well as the proposed step-wise implementation process are the foundation of the future blockchain-based safety surveillance system for medical devices.
- A solid knowledge of the current challenges and needs of the medical device industry, and continuous collaboration with blockchain technology experts will ultimately lead to the successful implementation of blockchain in the postmarket surveillance of medical devices.

across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks [6]. Blockchain is a technology based on public secure communication to track historical transactions related to distributed patient records. For example, Blockchain technology can offer efficient safety data exchange while maintaining data privacy, integrity and accessibility. This new technology could make available substantial quantities of anonymous PMS data from different sources (spontaneous reports, medical device registries, nonstandard data sources).

Blockchain enables multiple parties within a network to share a single ledger, which all parties can trust as valid. Each new piece of data (transaction) is included in a 'block', each block containing a hash of the prior block, connecting it to its predecessor and creating a chain of blocks – or blockchain. The network timestamps transactions by hashing them into a continuous chain of hash-based proof-of-work, creating a record that cannot be altered without redoing the proof-of-work [7]. These recorded transactions may be used to support currencies and payments but also safety data [8] (see Table 1). A node that is part of this network has to verify each new transaction to ensure its completeness. As each transaction in a block of a blockchain is verified by all of the nodes in the network, it becomes more immutable with every block added to the chain. The diagram below shows the workflow of the blockchain process (as shown in Figure 1). There are different levels of verification of ledgers. A public blockchain has ledgers that can be viewed by anyone, and anyone can verify and add a block of transactions to the blockchain [9]. A private blockchain allows only specific individuals in the organizations to verify and add transaction blocks but everyone on the internet is generally allowed to view them, depending on the type of blockchain [10]. Consortium: only a specific type of group within the organization (such as banks) can verify and add transaction but the ledger can be opened or restricted to the selected group [11].

Table 1. Key features of blockchain.

Key features	Functionality Description
Immutable	Blockchain is an immutable record that is distributed across multiple computers. The computers in the system compete to have the ability to add a new block (mining). Each block contains the prior block's hash. The blocks become reserved forever, and cannot be altered easily without having control of more than 51% of the nodes simultaneously.
Distributed	Blockchain does not have a controlling authority of the data. Participants prove themselves through Proof of Work or Proof of Stake. The data can be accessed, and updated on multiple computers.
Transparent	The data on blockchain is transparent to users, and can be further updated easily. The transparent nature of blockchains prevents data from being modified.
Autonomy	Each node on the blockchain system can store, transfer, and update the data securely, without any external interference.
Open Source	Blockchain offers an open source access to all the stakeholders connected to the network.
Anonymity	As data transfers from one node to another node, the identity of the individual during the data transfer remains anonymous.

3. Challenges related to adequate postmarket surveillance of medical devices

The following issues have been identified as challenges associated with implementation of adequate postmarket surveillance of medical devices:

3.1. Security & exchange of data

With a growing number of new technologies that connect medical devices, there is a potential for hacking of PMS data, which should be prevented [2,3]. A secure environment for data exchange is required to ensure rapid sharing with appropriate stakeholders. The timely exchange of PMS data throughout the different PMS data sources and PMS documents is one of the main challenges associated with the safety signal detection process for medical devices. The failure to promptly identify safety issues associated with marketed medical devices has recently led to public health scandals [12,13].

3.2. Medical device traceability

The identification of the root cause of the adverse event is crucial for a robust PMS system. In order to identify the root cause, the evaluation of the medical device sample is key to isolate the failure mode associated with the event, and is often lacking [4].

3.3. Counterfeit

Counterfeiting medical devices is a well-known threat to patient safety [14]. To address this issue, there has been an increasing regulatory demand for more information about the medical device origin [1].

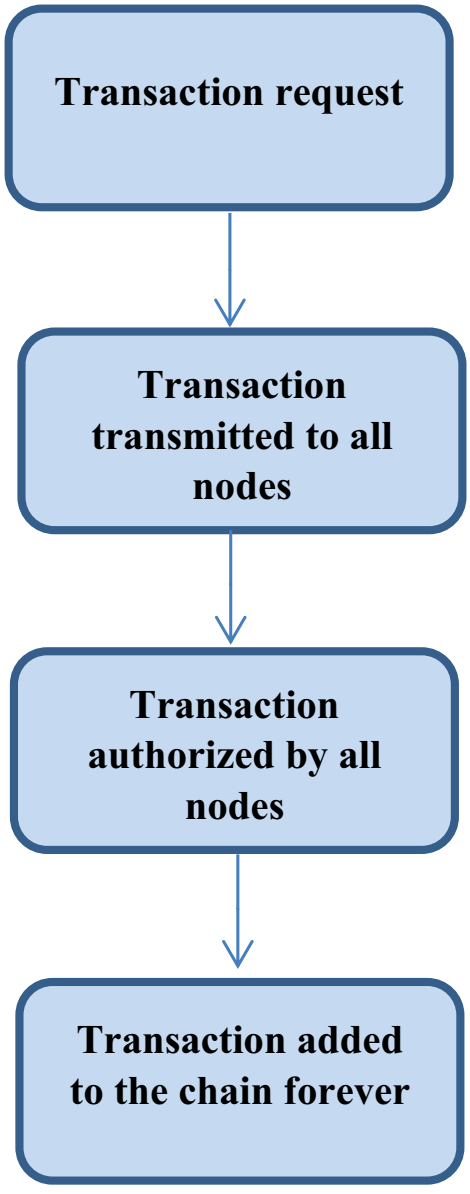

Figure 1. Workflow of the blockchain process.

3.4. Regulatory actions

To execute regulatory actions related to safety, it is required to quickly identify the location of all the medical devices in the market, which requires a Unique Device Identifier (UDI) [4].

3.5. Standardization

One of the main challenges during the safety signal detection of medical devices is the lack of standardization and harmonization of PMS data sources. Each PMS data source contains different content and uses a different methodology to store the data [3]. Two of the main types of medical device PMS data sources are Spontaneous Reporting Systems (SRS) and medical device registries. These two data sources have its own benefits and limitations:

- Spontaneous Reporting Systems: SRS are reactive systems that contain reports of patient harms and product problems collected from healthcare professionals, patients, healthcare authorities and manufacturers whether reported directly or through published articles. SRS are organized based on the relationship between medical devices and events. The data collection cover large populations and their processing is centralized normally in a repository or database where they are available for assessment [15,16,17,18,19]. Nevertheless, SRS suffer from different limitations including: lack of harmonized global standard data set for reporting which makes integration of data from different databases challenging [3,20], difficulty to determine root causes for individual events conclusively due to limited information and no access to the actual device, with a large part of investigation results being inconclusive [4], missing and incomplete data that impact the evaluation of the case, underreporting and over-reporting where medical devices with well-known adverse event/product problems are more likely to be reported than other medical devices based on influence from social network, or media coverage [21].
- Medical Device Registries: A medical device registry is defined as an 'organized system with a primary aim to increase the knowledge on medical devices contributing to improve the quality of patient care that continuously collects relevant data, evaluates meaningful outcomes and comprehensively covers the population defined by exposure to particular device(s) at a reasonably generalizable scale (e.g. international, national, regional, and health system)' [22]. Medical device registries typically contain valuable information such as medical device information, diagnoses, medications, medical narratives and surgical interventions. Unlike spontaneous reports, medical device registries are not restricted to patients experiencing medical device product problems or patient harms. Therefore, medical device registries data provide some advantages that can be used to complement the more traditional PMS data sources (SRS), particularly confirmatory studies and the possibility to perform active PMS [23,24]. Although the use of medical device registries presents many advantages, it also presents certain challenges:
  - o Lack of standardization: the characteristics of the registry might vary across countries with differences in granularity, consistency and quality of data, duration of longitudinal follow-up, attrition rates, data privacy standards, regulation, ability and level of information exchange [25]. This lack of standardization between the different registries may lead to a possible delay before PMS data from international registries is collected and consolidated, eventually causing a delay in safety signal verification [22].
  - o The lack of use of a harmonized UDI and nomenclature codes impacts the analysis of device outcome information from the registry [26].

3.6. User training

A key contributing factor to adverse events with medical devices is the user error [3]. Development of appropriate risk

mitigation activities, mainly training, is essential to ensure safe handling of medical devices.

4. Opportunities for use of blockchain technology to address challenges in medical device PMS system

For medical device PMS we see potential for a public permissionless blockchain, and for a private permissioned blockchain, which may address several of the challenges that have been mentioned above (see Table 2).

4.1. Medical device traceability

Blockchain technology may very well support the global implementation of UDI. Blockchain enables the recording of data of all production and ongoing usage or maintenance. Its immutable and reliable workflow will support the medical device manufacturers with complete traceability and provide evidence on any safety issue associated with the specific medical device. This type of technology is becoming more relevant following the additional traceability requirements (Articles 25 and 27 of the EU MDR) [1], which will come into place in May 2021. The new regulation requires an UDI to be included on all product packaging in both human-readable and machine-readable form. Annex VI of the MDR discusses the usage of automatic identification and data capture tools such as QR codes or bar codes, which could eventually be used in conjunction with blockchain technology. Machine-readable information can be encoded within a bar code, and potentially include access to a blockchain traceability system within the one bar code [27]. The blockchain traceability tool serves in the recording of each step of the supply chain and interaction with the product. Any economic operator, who is engaged with that medical device, would have access to the blockchain and thus would be able to review the interactions of that medical device. This activity will make important data efficiently available to the health authorities. By reading the blockchain, end-recipients could autonomously confirm that a medical device is genuine by confirming its authenticity against the UDI database and through the supply chain. Article 28 of the new MDR requires that the UDI database warrants 'maximum accessibility to information stored therein, including multi-user access' and which shall 'validate, collate, process and make available to the public (the information)'. The regulation requires 'appropriate methods … for validation of the data provided' and that 'manufacturers … periodically verify the correctness of all of the data relevant to devices they have placed on the market' [1]. A blockchain-based repository could provide some of the functionalities the regulators require.

Table 2. Applications of blockchain technology in PMS of medical devices.

Gap in Medical Device PMS	How blockchain can address this gap
Medical device traceability	Blockchain technology could support the global implementation of UDI.
Regulatory actions and counterfeit	Blockchain can be used to track and monitor regulatory actions related to the market release of devices, and will also help to verify medical device counterfeiting.
Security, standardization and exchange of PMS data	Blockchain can provide a secure real time exchange of PMS data, which could be part of the distributed ledger of an approved blockchain. The integration of blockchain in PMS has the potential to standardize the content and the format of PMS data sources, and create a more efficient protected PMS data exchange process.
User errors	Blockchain can fastly identify different type of user errors in a faster manner, and find the training required to address the type of user error.

4.2. Regulatory actions & counterfeit

The global adoption of UDI [4], and blockchain technology could improve the efficiency of the regulatory action coordination process by tracking all the medical devices that are on the market to ensure fast and efficient removal from the market. Through its ability to track all transactions, blockchain technology is able to monitor every stage of the medical device supply chain. Blockchain will reinforce data integrity and improve medical device traceability across the supply chain, and will also help to verify medical device counterfeiting.

4.3. Security, standardization & exchange of PMS data

The immutability of Blockchain supports fraud detection by prohibiting any replication or alteration in the transaction, leading to a transparent, reliable and secure record. Blockchain may support a more proactive approach to collect PMS data (spontaneous reports, registries, nonstandard data sources, etc.), by allowing to directly obtain data without the need to 'actively report' the adverse event; e.g. a patient entry in a medical device registry is completed, or a healthcare professional enters information on an adverse event related to a device in an electronic health record. This could become a block of data that is shared when the relevant data fields are entered, without the need to actively choose to report an adverse event. This initiative could lead to an increased amount of postmarket data with limited human interaction that would eventually lead to better quality of collected PMS data.

Blockchain provides a distributed secure framework for any exchange of safety data. This type of framework is not part of a central group 'controlling' its accesses and, therefore less likely to be affected by a cyberattack. The nature of distribution of blockchain could help to maintain PMS data in a more systematic way, and provide permanent secure storage of medical device PMS data through new storage solutions which enable users to store PMS data in a platform that live forever on a blockchain, all while keeping the speed high and a low monetary cost low.

The PMS data could be part of the distributed ledger of an approved blockchain. The integration of blockchain in PMS has the potential to standardize the content and the format of PMS data sources, and create a more efficient protected PMS data exchange process [28], guarantee data integrity and transparency, and eliminate any human intervention; from data creation to data retrieval. The

involvement of many and unrelated participants strengthens the integrity of the chain by decreasing the risk of collusion to modify data. This risk is reduced due to the fact that consensus is mandatory to change the chain. Although the PMS data on a public blockchain would be secure and the identity of the participants would be pseudonymized, the data would not be private. Instead, data would be transparent for all participants to review. To enable privacy, 'private' blockchains should be developed, so that only certain stakeholders can participate, review and modify the blockchain. This type of 'private' blockchains could be used for the exchange of PMS data between the different stakeholders involved in the process of safety evaluation of medical devices.

4.4. User errors

Blockchain technology can support the identification of safety issues for software devices related to user error in a faster manner informing the manufacturer on the type of user error and identifying the training required to address the type of user error.

5. Challenges in use of blockchain technology

In order to ensure the successful implementation of blockchain in the PMS process of medical devices, it is crucial to understand the challenges associated with the use of this new technology (Table 3).

5.1. Security and privacy of data

Blockchain provides a higher level of security as the need for a third-party involvement in the completion of the transaction of safety data is eliminated. Nevertheless, the data becomes vulnerable to potential privacy and security risks as the mechanism of blockchain allows the entire community of users, rather than a single third party, to verify the records in a blockchain architecture [5]. Since all nodes are able to view the data transmitted by one node, data privacy cannot be ensured. Absence of a third party for approval requires the patient to pick one representative that can view his information, in the case of an emergency. This representative may allow other individuals to access the records of the same patient, which may generate a significant data privacy and security risk. The alternative option would be to create high-security mechanisms to the data, but this would result in obstacles in transferring the data from one block to another and, thus, lack of access of data. In addition, blockchain networks are vulnerable to a kind of security breach known as 51% attack [29,30]. This attack consists of a group of miners that collectively own more than 50% of the nodes in a blockchain network and collaborate to alter the blockchain data. The miners get an authority of the network and could prevent the completion of any new transactions by not authorizing them with the consent. Five cryptocurrencies have recently been a victim of this attack [31]. Lastly, another challenge associated with the use of blockchain with PMS is that a patient record might have sensitive data that is unsuitable to be on the blockchain [32]. To address these challenges, we suggest to generate a private PMS data permissioned blockchain with a proof-of-authority consensus mechanism, where only a restricted number of designated and audited participants have authorization to validate transactions and add them to the PMS data blockchain ledger. Alternatively, we could recommend a reliable decision-making setting: for example, using the blockchain-based system called MedRec [33], patients/healthcare professionals/manufacturers/health authorities can approve the addition of new members to the private blockchain, protect and identify the members of the PMS community responsible for approving changes, and govern the sharing between the different stakeholders. This enables members of the PMS community to add a new record associated with a specific patient, and patients can approve sharing of records between different stakeholders. There is prioritization of use in all user-stakeholder interactions, and this will provide a single database to review any updates to patients' medical history. In addition to enhance PMS stakeholders control over PMS data sharing, this proposal could also remove one of the main obstacles during exchange of PMS data which is data reliability [28].

Yet another solution would be to ensure full data privacy to participants during the PMS data transaction, while still being able to validate the authenticity of the transaction. However, some of the participants in our private blockchain could be medical device manufacturers. The conventional blockchain application would allow participants to obtain sensitive private data about their competitors. To eliminate any risk of competitors acquiring sensitive information about each other, our PMS private blockchain should build a zero-knowledge proof algorithm mechanism ensuring that competitors cannot see the transaction data of their competitors, while allowing transactions to be validated [34].

5.2. Manage data storage

Another challenge is the management of data storage capacity. The traditional web and its data storage systems are fragile and liable to potential data losses. Contrary to what happens with the traditional centralized data storage systems, blockchain offers a distributed tool to store the data. Blockchain is designed to track and complete the transaction of data. However, PMS has a large amount of data that must be stored on a regular basis [35]. All the PMS data in the blockchain should be available to all the nodes in the chain, which needs a great storage capacity [6,36]. Due to growing number of PMS databases, the rapidity of event searching and editing can be low and this could represent a challenge, which is highly unsuitable for the PMS data transactions where speed is crucial. Therefore, to address this challenge, a blockchain solution needs to have huge storage capacity in order to be scalable [37]. As an example; this solution could be related to the development of a platform that enables the user to store PMS data that live forever on a blockchain, all while keeping high speed and a low monetary cost.

Table 3. Challenges and recommendations associated with the use of blockchain technology.

	Challenge	Recommendation	Owner
Security and Privacy Data	Blockchain lets the entire community, rather than a single third party, verify the records in a blockchain architecture. The PMS data becomes vulnerable to potential privacy and security risks.	Generate a private PMS permissioned blockchain with a proof-of-authority consensus mechanism.	IMDRF, HA's, manufacturers, hospitals
Manage data storage	Event searching and editing can be slow, which is highly unsuitable for PMS data transactions where speed is crucial.	A blockchain solution needs to have huge storage capacity in order to be scalable.	IMDRF, HA's
Interoperability issues: PMS data exchange	Current PMS databases are off-line, centralized, local databases with a very different architecture compared to blockchain, which is distributed and in the cloud. Most of global regulations still require the exchange of PMS data to be controlled by central health authorities, and they also mandate to comply with data privacy requirements when completing transactions of PMS data.	Use of a private PMS permissioned blockchain with a proof-of-authority consensus mechanism. Develop new global guidances to ensure blockchain implementation. All current PMS data sources converted to a blockchain system.	IMDRF, HA's, manufacturers, hospitals
Standardization challenges	PMS data exchange systems are not fully integrated.	Integration of PMS data exchange systems and development of international standardized documents to scrutinize the shared data in terms of size, nature, and format of the data exchanged in blockchain applications.	HA's, IMDRF
Behavioral challenges	Blockchain technology is still developing, and therefore, faces behavioral challenges.	Develop educational materials to disseminate, and identify the strengths and opportunities of blockchain technology in the medical device industry.	HA's, Hospitals, Manufacturers
Monetary cost	The cost of transition to full IT systems with blockchain technology could be significant.	The PMS stakeholders should financially support this technological shift.	HA's, Hospitals, Manufacturers

5.3. Interoperability issues – exchange of PMS data

PMS databases are off-line, centralized, local databases with a very different architecture as compared to the blockchain technology, which is distributed and decentralized In order to implement blockchain technology, an efficient PMS database capable of enabling interoperability among the different PMS stakeholders will need to be set up [28]. One of the main challenges of this implementation is that most of the global regulations still require the exchange of PMS data to be controlled by central health authorities, and they also mandate to comply with data privacy requirements when completing transactions of PMS data [27]. These challenges could be mitigated with the use of a private PMS permissioned blockchain with a proof-of-authority consensus mechanism, where only a restricted number of designated and audited participants (health authorities, manufacturers and reporting facilities) have authorization to validate transactions and add them to the PMS data blockchain ledger. New global guidance need to be developed to ensure successful blockchain implementation, and that all current PMS data sources would need to be converted to the new private PMS permissioned blockchain system.

5.4. Standardization challenges

The integration of blockchain in PMS has the potential to standardize protected PMS data exchange in a more efficient manner [28]. However, blockchain technology is still in its beginning, and its practical implementation in PMS of medical devices will have standardization challenges. Health Authorities should develop international standardized documents to scrutinize the shared data in terms of size, nature, and format of the data exchanged in blockchain applications. The lack of a harmonized data set could lead to each country/region generating a block with a different data set. Blockchain applications will not deliver value if the existing PMS data exchange systems are not fully integrated, and all business rules are followed and automatically enforced.

5.5. Behavioral challenges

In addition to the mentioned technical challenges, blockchain technology is still developing, and therefore, faces behavioral challenges, like cultural change. Although the medical device industry is gradually moving toward digitization, there is still a lot that needs to be changed in order to totally transform the current heavy-administrative PMS data exchange tools to this blockchain technology, which has not yet been validated in PMS data exchange. Convincing doctors, patients, manufacturers and health authorities to switch from paperwork to making use of technology will not be an easy process and will take time and training. Due to its low adoption rate in the healthcare industry in general, the technology and regulations offered are relatively untrusted [37]. The stakeholders involved in PMS process for medical devices should develop educational materials to disseminate, and identify the strengths and opportunities of blockchain technology in the medical device industry.

5.6. Monetary cost

Due to the limited talent that currently exists to write the blockchain infrastructure, it is expensive to get the data on the block, and then for a certain number of blocks to be created to ensure our block is irrevocable. Therefore, since PMS data exchange should be completed in a timely manner to ensure early identification of safety risks, we may need to speed up the transaction time (number of transactions per second). In order to do that, we may need to pay more transactional charges (which can get expensive, depending on the network availability). The cost to implement this new technology in the PMS system should be taken into consideration. Some hospitals are not fully computerized and would not be able to share data with each other (e.g. if they do not belong to the same consortium). A major shift in IT systems will need to occur and the cost of that transition to full IT systems with blockchain technology could be significant. The different PMS stakeholders (health authorities, manufacturers and hospitals) should financially support this technological shift. Some of them have already started exploring the use of this new technology; the EU Commission announced the launch of an EU Blockchain Observatory and Forum to monitor PMS data, evaluate trends, and address emerging issues [38]. The project is part of an initiative to develop a standardized approach to blockchain for the EU [39] that could potentially extend to the Eudamed database in the future.

6. Implementation strategy of the new private PMS data permissioned blockchain: 10-year plan

In order to successfully implement the new private permissioned blockchain in PMS of medical devices, it is important to design a step-wise implementation strategy with clear goals, timelines, roles and responsibilities. The entire project should be funded by a consortia comprised of the different PMS stakeholders (Health Authorities, Manufacturers and Hospitals) and coordinated by IMDRF. Each member is to pay yearly fees to economically support the changes required to build and implement the new PMS system of medical devices based on the new private PMS data permissioned blockchain.

6.1. Phase I- standardization (1st – 2nd year)

The International Medical Device Regulatory Forum (IMDRF) is a group of medical device regulators (Australia – TGA, Brazil – ANVISA, Health Canada, China FDA, European Commission, Japanese PMDA and MHLW, Russian Ministry of Health, Singapore – HSA, South Korea – Ministry of Food and Drug Safety, US FDA) that have voluntarily come together to harmonize the regulatory requirements for medical products that vary from country to country. IMDRF will start a project to standardize the different PMS requirements across jurisdictions. In order to ensure that PMS data will be captured consistently in the new

blockchain system, IMDRF will coordinate the standardization efforts required for the implementation of the new system. IMDRF will need to negotiate with the different PMS stakeholders (HAs, hospitals and manufacturers) to reach consensus on the identification of the PMS data sources, the adverse event reporting criteria, the adverse event coding dictionaries, and the device identification systems that will eventually be used globally in the new private permissioned blockchain.

6.2. Phase II – new global PMS database & private data permissioned blockchain (3rd – 4th year)

After agreeing and deciding on the global PMS requirements and the new global adverse event reporting dataset, IMDRF will start working with a technology partner to develop the new PMS global database software that will use a new private data permissioned blockchain with proof-of-authority to verify every PMS data transaction. Governance will need to be developed regarding participation in and the use of the new global PMS database. The principles governing transparency, confidentiality, supervision and regulatory reporting of the new database, as well as the governing agreements of the private data permissioned blockchain will need to be agreed by all parties and documented.

6.3. Phase III – US pilot (5th year)

After agreeing and deciding on the global PMS requirements, IMDRF will start a pilot in the US for the implementation of the new private permissioned blockchain. Manufacturers will need to ensure the follow through of the use of blockchain in the supply chain management process to guarantee medical device traceability using blockchain, and convert the existing manufacturer's PMS data sources (SRS, registries …) to blockchain. Hospitals and Health Authorities participating in the pilot will need to ensure the use of blockchain during the PMS data exchange process by converting the existing safety data sources to blockchain. The pilot should be championed by the IMDRF with the participation of one health authority (the FDA), 3 US medical device manufacturers and 3 US hospitals. The goal of this pilot will be to demonstrate blockchain's ability to connect different systems and administrations, in order to track a common dataset of product traceability and patient data, and show how blockchain could potentially improve PMS of medical devices by reducing the time it takes to alert the supply chain of a medical device recall, and reducing the time it takes to share PMS data across the different PMS stakeholders. IMDRF will need to provide a technology partner and a consulting group that will work with the manufacturers, hospitals and FDA to provide the tools, guidance and support required during the pilot. The technology partner will provide the PMS software based on the agreed standardized reporting dataset from Phase I. This software will use the blockchain infrastructure for the data transaction verification. The consulting group will support the pilot participants with training, follow-up, and most importantly will ensure that the data is well and correctly captured. Lessons learned from the pilot will be shared with all the IMDRF members.

6.4. Phase IV – global pilot (6th year)

After the successful completion of the US pilot, a second pilot will start on a global level. Again, the IMDRF should champion this second pilot, with the participation of 3 health authorities (the FDA, European Commission, China FDA), 9 medical device manufacturers (3 from US, 3 from EU, and 3 from China) and 9 hospitals (3 from US, 3 from EU, and 3 from China). The goal of this pilot will be to address unanswered questions and challenges resulted from the US pilot, and demonstrate blockchain's ability to connect different systems and administrations globally, in order to track a common dataset of product traceability and patient data, taking into consideration the different local data privacy regulations, and show how blockchain could potentially improve PMS of medical devices. IMDRF will need to provide a technology partner and a consulting group that will work with the manufacturers, hospitals and national health authorities to provide the tools, guidance and support required during the pilot. Additionally, and given the global environment, such partner and consultants will also aid in overcoming any cultural differences associated with the implementation of this new technology (language, technological differences per country, PMS data confidentialy requirements, etc.). Lessons learned from the pilot will be shared with all the IMDRF members. If they find, at any point during or after the pilot, additional areas of focus to ensure the successful implementation globally or if any flaws or limitations are identified, the timeline of the pilot is subject to change and extension.

6.5. Phase V – new global blockchain regulations (7th – 8th year)

After the successful completion of the global pilot, each of the local health authorities coordinated by the IMDRF will develop and publish local regulations and guidelines for the local hospitals and local manufacturers to ensure successful implementation of the blockchain system by the global agreed GO-LIVE date. The regulations and guidelines will contain direction on data privacy management based on the corresponding local confidentiality regulations. The documents will also include the transition period for the global implementation.

6.6. Phase VI – transition period (9th – 10th year)

During the 2-year transition period, the PMS stakeholders should work with the appropriate technological partner and consulting group (if required) to implement the GO-LIVE date. All hospitals, manufacturers and health authorities will have two years to convert the SRS and medical registries to the new private PMS data permissioned blockchain. The local health authorities will provide local technological and training support to ensure the different country PMS stakeholders will be ready to implement the new blockchain system by the agreed due date.

6.7. Phase VII – GO LIVE

After the 2-year transition period and the GO-LIVE date, a dedicated team within the IMDRF group will monitor any challenges associated with the usage of the new system. This group will provide technological and training support, when required. The local health authorities will need to enforce the use of this technology across the different local PMS stakeholders, and ensure adherence to the new private PMS data permissioned blockchain regulations during the periodic inspections of the stakeholder's PMS system.

7. Conclusion

Blockchain technology has great potential. Its development coincides with the timing that PMS for medical devices needs to be implemented, which offers a great opportunity and synergy.

Our proposed solutions can only be successfully implemented if they are established on the basis of a solid knowledge of the current challenges and needs of the medical device industry, and in continuous collaboration with a blockchain technology expert. This expert will eliminate the potential failure of the new system due to a lack of understanding of the performance of blockchain and its impact on PMS process.

This new technology has the potential to support a more efficient approach for the PMS of medical devices, which could offer many advantages to the different stakeholders involved in the process, such as supporting new regulatory initiatives.

8. Expert opinion

In order to guarantee the successful implementation of blockchain in the PMS process of medical devices, it is vital to start working on robust initiatives to address the challenges associated with the use of this new technology.

8.1. What should the PMS community focus on? prioritization

The existing resources available to the different stakeholders involved in PMS of medical devices are limited. There is a need to identify the main priorities the PMS stakeholders should focus on:

8.1.1. Data privacy

Blockchain provides a higher level of security as the need for a third-party involvement in the completion of the transaction of safety data is eliminated. Nevertheless, the data becomes vulnerable to potential privacy and security risks as the mechanism of blockchain allows the entire community of users, rather than a single third party, to verify the records in a blockchain architecture. PMS resources should focus on the design of solutions that ensure full data privacy to participants during the PMS data transaction, and also continue to guarantee the validation of the authenticity of the transaction.

8.1.2. Data storage

Contrary to the traditional centralized data storage systems, the blockchain solution offers a distributed tool to store its data. PMS is subject to large amounts of data, which must be stored on a regular basis in the blockchain and should be available to all the nodes in the chain. In order to ensure the scalability, success and availability of our blockchain, a large storage capacity will need to be provided to store all data.

8.1.3. Data exchange

Current PMS databases are off-line, centralized, local databases with a very different architecture as compared to the blockchain technology, which is distributed and decentralized. In order to implement blockchain technology, an efficient PMS database capable of enabling interoperability among the different PMS stakeholders will need to be set up. One of the main challenges of this implementation is that most of the global regulations still require the exchange of PMS data to be controlled by central health authorities. New global guidances need to be developed to ensure successful blockchain implementation, and that all current PMS data sources would need to be converted to the new PMS global database software that will use the new private PMS permissioned blockchain system.

8.1.4. Data standardization

The lack of a standardized data set could lead to each country/region generating a block with a different data set. Blockchain applications will not deliver value if the existing PMS data exchange systems are not fully integrated, and all business rules are followed and automatically enforced. International standardized documents to scrutinize the shared data in terms of size, nature, and format of the data exchanged in blockchain applications will need to be developed.

If correctly implemented, blockchain technology has the potential to solve some of the current challenges associated with PMS of medical devices, and will be crucial in the future in defining the pillars of the new surveillance system.

Funding

This paper was not funded.

Declaration of interest

The authors have no relevant affiliations or financial involvement with any organization or entity with a financial interest in or financial conflict with the subject matter or materials discussed in the manuscript. This includes employment, consultancies, honoraria, stock ownership or options, expert testimony, grants or patents received or pending, or royalties.

Reviewer disclosures

Peer reviewers on this manuscript have no relevant financial or other relationships to disclose.

ORCID

Josep Pane http://orcid.org/0000-0003-0869-2833
Katia M.C. Verhamme http://orcid.org/0000-0001-8162-4904
Miriam C.J.M. Sturkenboom http://orcid.org/0000-0003-1360-2388

References

Papers of special note have been highlighted as either of interest (•) or of considerable interest (••) to readers.

1. Regulation (EU). 2017/745 of the European Parliament and of the Council of 5 April 2017; 2017.
2. Pane J, Francisca RDC, Verhamme KMC, et al. EU postmarket surveillance plans for medical devices. Pharmacoepidemiol Drug Saf. 2019;28(9):1155–1165.
3. Pane J, Coloma PM, Verhamme KMC, et al. Evaluating the safety profile of non-active implantable medical devices compared with medicines. Drug Saf. 2017;40(1):37–47.
   • **Paper reports results of a review of challenges associated with the safety evaluation of medical devices that was included in the current manuscript.**
4. Pane J, Verhamme KMC, Rebollo I, et al. Descriptive analysis of postmarket surveillance data for hip implants. Pharmacoepidemiol Drug Saf. 2020;29:380-387.
5. Mackey T, Kuo T, Gummadi B, et al. "Fit-for-purpose?" - challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Med. 2019;17:68.
   • **Paper reports results of a review of opportunities for applications of blockchain technology in healthcare that was included in the current manuscript.**
6. Pirtle C, Ehrenfeld J. Blockchain for healthcare: the next generation of medical records? J Med Syst. 2018;42(9):172.
7. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system cryptovest; 2008. Available from: https://bitcoin.org/bitcoin.pdf
   •• **The original Satoshi Nakamoto's paper that provides an in-depth overview of the bitcoin and the blockchain technology.**
8. Siyal A, Junejo A, Zawish M, et al. Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. Cryptography. 2019;3(1):3.
9. Xu L, Shah N, Chen L, et al. Enabling the sharing economy:Privacy respecting contract based on public blockchain. In: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. ACM; Abu Dhabi, United Arab Emirates. 2017. p. 15–21.
10. Dinh TTA, Wang J, Chen G, et al. Blockbench: A framework for analyzing private blockchains. In: Proceedings of the 2017 ACM International Conference on Management of Data. ACM; Chicago, USA. 2017. p. 1085–1100.
11. Mohanta BK, Jena D, Panda SS, et al. Blockchain technology: a survey on applications and security privacy challenges. Internet Things. 2019;8:100107.
12. Health, Canada. Metal-on-metal hip implants - information for orthopaedic surgeons regarding patient management following surgery - for health professionals; 2012. Available from: http://healthycanadians.gc.ca/recall-alert-rappel-avis/hc-sc/2012/15835a-eng.php
13. New York Daily News. EU to tighten medical controls after breast implant scandal; 2012. Available from: http://www.nydailynews.com/life-style/health/eu-tighten-medical-controls-pip-breast-implant-scandal-article-1.1169444
14. Europe M. Keeping up with counterfeiters: the battle against counterfeit medical devices; 2018. Available from: https://www.medtechintelligence.com/column/keeping-up-with-counterfeiters-the-battle-against-counterfeit-medical-devices/
15. Laskey W, Awad K, Lum J, et al. An analysis of implantable cardiac device reliability. The case for improved postmarketing risk assessment and surveillance. Am J Ther. 2012;19(4):248–254.
16. DiBardino DJ, McElhinney DB, Kaza AK, et al. Analysis of the US food and drug administration manufacturer and user facility device experience database for adverse events involving amplatzer septal occluder devices and comparison with the society of thoracic surgery congenital cardiac surgery database. J Thorac Cardiovasc Surg. 2009;137(6):1334–1341.
17. Clark KK, Sharma DK, Chute CG, et al. Application of a temporal reasoning framework tool in analysis of medical device adverse events. AMIA Annu Symp Proc. 2011;2011:1366–1371.
18. Tambyraja RR, Gutman MA, Megerian CA. Cochlear implant complications: utility of federal database in systematic analysis. Arch Otolaryngol Head Neck Surg. 2005;131(3):245–250.
19. Tremaine AM, Avram MM. FDA MAUDE data on complications with lasers, light sources, and energy-based devices. Lasers Surg Med. 2015;47(2):133–140.
20. European Commission. JRC initiative on signal detection and management. Open Conceptual Framework & Integrated Approach; 2017.
21. Hazell L, Shakir S. Under-reporting of adverse drug reactions. Drug Saf. 2006;29(5):385–396.
22. IMDRF. Methodological principles in the use of international medical device registry data; 2017. (Contract No.: IMDRF/Registry WG/N42FINAL:2017).
23. Hauser RG, Mugglin AS, Friedman PA, et al. Early detection of an underperforming implantable cardiovascular device using an automated safety surveillance tool. Circ Cardiovasc Qual Outcomes. 2012;5(2):189–196.
24. Duggirala HJ, Herz ND, Caños DA, et al. Disproportionality analysis for signal detection of implantable cardioverter-defibrillator-related adverse events in the food and drug administration medical device reporting system. Pharmacoepidemiol Drug Saf. 2012;21(1):87–93.
25. OECD. Non-medical determinants of health; 2016. Available from: https://www.oecd-ilibrary.org/social-issues-migration-health/data/oecd-health-statistics/oecd-health-data-non-medical-determinants-of-health_data-00546-en
26. IMDRF. Unique device Identification (UDI) of medical devices; 2013. (Contract No.: IMDRF/UDI WG/N7FINAL:2013).
27. Torne L. Blockchain: the answer to medtech traceability; 2018. Available from: https://medtech.pharmaintelligence.informa.com/MT122222/Blockchain-The-Answer-to-Medtech-Traceability
28. Stone D. Blockchain: the challenges and opportunities in healthcare; 2018. Available from: https://www.divurgent.com/knowledge-center/blockchain-in-healthcare/
29. Investopedia. 51% attack; 2019. Available from: https://www.investopedia.com/terms/1/51-attack.asp
30. Palmer D. The vertcoin cryptocurrency just got 51% attacked - again coindesk; 2019. Available from: https://www.coindesk.com/the-vertcoin-cryptocurrency-just-got-51-attacked-again
31. Hertig A. Blockchain's once-feared 51 percent attack is now becoming regular; 2018. Available from: https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular
32. Linn LA, Koo MB. Blockchain for health data and its potential use in health it and health care related research. ONC/NIST Use of Blockchain for Healthcare and Res Workshop; Gaithersburg, USA. 2016.
33. Ekblaw A, Azaria A, Halamka JD, et al. A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. IEEE; Washington DC, USA. 2016.
34. Mattke J, Maier C, Hund A, et al. How an enterprise blockchain application in the U.S. pharmaceuticals supply chain is saving lives. MIS Q Executive. 2019;18(4):245–261.
35. Esposito C, De Santis A, Tortora G, et al. Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 2018;5(1):31–37.
36. Bennett B. Blockchain HIE Overview: A Framework for Healthcare Interoperability. Telehealth and Medicine Today. 2018:2(3).
37. McKinley L, Pithouse D, Sanders J. Blockchain: background challenges and legal issues: DLA piper publications; 2016. Available from: https://www.dlapiper.com/en/denmark/insights/publications/2017/06/blockchain-background-challenges-legal-issues/
38. European Commission. European commission launches the EU blockchain observatory and forum; 2018. Available from: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_521
39. European Commission. Blockchain technologies; 2019. Available from: https://ec.europa.eu/digital-single-market/en/blockchain-technologies