Blockchain technology in the healthcare sector: overview and security analysis

Nour El Madhoun, Badis Hammi

Blockchain Technology in the Healthcare Sector: Overview and Security Analysis

Nour El Madhoun*†, Badis Hammi ‡
* LISITE Research Lab, Institut Supérieur d'Electronique de Paris (ISEP), 92130 Issy-les-Moulineaux, France
† Sorbonne Université, CNRS, LIP6, F-75005 Paris, France
‡ SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, France
nour.el-madhoun@isep.fr; badis.hammi@telecom-sudparis.eu

***Abstract*—Today, the healthcare sector is suffering from multiple security vulnerabilities that make it vulnerable to various types of cyberattacks. Therefore, robust security solutions need to be implemented in order to resolve these vulnerabilities. In this context, blockchain technology has emerged as a promising solution in several sectors, including the healthcare sector. It ensures enhanced security and greater transparency. It also boosts patient confidence and optimizes operational efficiency. In this paper, we first present an overview of the main classic healthcare applications: medical records management, traceability of medicines, and research and clinical trials. We then present a detailed analysis of the critical security vulnerabilities threatening these applications. Afterwards, we explain how blockchain technology can help to address these vulnerabilities. Finally, we discuss the various possible methods that aim to prevent traditional blockchain-related attacks in these healthcare applications and how blockchain technology is impacting and transforming the healthcare sector.**

***Index Terms*—Attack, Blockchain, Confidentiality, Healthcare, Integrity, Privacy, Security.**

I. Introduction

The healthcare sector is currently facing a number of security vulnerabilities that represent major risks for the confidentiality, integrity and availability of healthcare data. These vulnerabilities and risks make the healthcare sector particularly vulnerable to numerous types of cyberattacks. Consequently, the implementation of robust security solutions is required in order to effectively protect the sensitive data and maintain the continuity of the healthcare services [1] [2].

Blockchain technology has demonstrated its full potential as a valuable solution to a variety of security challenges in several sectors and particularly in the healthcare sector. It has a number of intrinsic properties such as decentralization, immutability and transparency, and other, that offer considerable advantages in terms of enhanced security, protection of data from unauthorized modifications, and complete traceability of operations while reinforcing the confidence of patients and healthcare professionals [3][4][5].

We summarize the significant contributions of this paper as follows:

1) We analyze the critical security vulnerabilities in the three main healthcare applications: medical records management, traceability of medicines and research and clinical trials.
2) We provide a detailed analysis on how the blockchain technology can contribute to face these security vulnerabilities.
3) We present an overview of the most common attacks targeting the blockchain technology and discuss how they can be avoided in the discussed healthcare applications.
4) We explore the impact and transformation of blockchain technology on the healthcare sector by examining the changes it offers in terms of security and innovation.

This paper is organized as follows. Section II presents our security analysis and begins with an overview of the three main classic healthcare applications. Section III focuses on how blockchain technology is impacting and transforming the healthcare sector. Finally, Section IV concludes the paper.

II. Security analysis of healthcare applications

A. Overview of the main healthcare applications

Blockchain technology can be applied to a plethora of healthcare applications. In this paper, we focus on the three main healthcare applications: medical records management, traceability of medicines, and research and clinical trials. This section presents how these applications are implemented traditionally, that is, without the integration of blockchain technology.

1) Medical records management: traditionally, medical records are managed through Electronic Health Records (EHR) or Electronic Medical Records (EMR) systems. These systems are designed to store and manage a patient's health information digitally. They technically operate on centralized databases that are managed either by individual healthcare institutions or by third-party providers. EMRs include data such as a patient's medical history, test results, diagnoses, treatments, prescribed medications and allergies. Access to these data is usually controlled by identity and access management systems that use logins and passwords to authenticate authorized users, such as nurses, doctors and administrative staff. EMR systems can also be interconnected with other medical infrastructures and systems such as pharmacies, laboratories and billing systems [6].

2) Traceability of medicines: traditionally, it relies on complex, multi-layered pharmaceutical supply chains. These systems use centralized databases to record and track medicines at each step, from manufacture to distribution to the patient.

Tracking is usually performed using batch numbers and barcodes that are scanned and recorded at each transfer point [7]. This allows to track the movement of medicines and manage stocks. Moreover, traceability systems can include mechanisms to monitor storage and transport conditions such as temperature [7]. The data collected is used to ensure regulatory compliance and for product recalls if necessary [8].

3) Research and clinical trials: traditionally, data are collected, stored and analyzed using a Clinical Data Management Systems (CDMS). CDMS systems collect data from a variety of sources such as direct observations, questionnaires, biological samples and measuring devices. These data are then processed and stored in a centralized database. The process often involves a manual input of data although Electronic Data Capture (EDC) devices are increasingly used to improve efficiency and reduce errors. Then, researchers employ statistical software to analyze the collected data, assessing the effectiveness, safety, and potential side effects of the treatments under study. Finally, participants' consent is managed using consent forms, which are often paper-based [9].

B. Security vulnerabilities

In this section, we present the security vulnerabilities that we have identified for the healthcare applications discussed above. Next, we assess how the integration of the blockchain technology helps to address these vulnerabilities. Afterwards, we introduce the most common attacks that target the blockchain technology. Finally, we exhibit the various prevention strategies that can be adopted to face these attacks when blockchain technology is adopted in the healthcare applications.

1) Security vulnerabilities in the medical records management:

Use of centralized storage: it makes medical records particularly vulnerable to Distributed Denial of Service (DDoS) attacks and system failures. Consequently, an attack on the central server or a failure can lead to total data unavailability, with a serious impact on the hospital's operations and medical decision-making, as healthcare professionals heavily depend on access to patient data.

Insecure access: the lack of robust security protocols such as strong encryption and authentication mechanisms exposes medical data to risks of intrusion. Consequently, this can lead to data violations by compromising the confidentiality and integrity of patient's information [1].

Lack of interoperability: the lack of standardized information systems across various healthcare institutions presents challenges in securely and efficiently sharing data. This lack of interoperability can actually lead to medical errors due to the use of incomplete or incorrect patient information. For this reason, fluid and precise communication between the different actors in the healthcare ecosystem is needed to ensure optimal patient care [10]

To support our point, we cite two examples:

(1) The attack on SingHealth (2018): it was a targeted and sophisticated cyberattack on the electronic medical records system of SingHealth, the largest healthcare group in Singapore. It exploited vulnerabilities in an electronic medical records database where attackers used phishing techniques to obtain the credentials of a single employee and then used these data to gain access to the whole system. The attack has compromised the personal data and prescriptions of almost 1.5 million patients, including the Prime Minister of Singapore. Furthermore, the investigation revealed that security measures were inadequate, particularly regarding the monitoring of suspicious activities and incident response [11].

(2) The WannaCry ransomware (2017): WannaCry is a ransomware that has infected hundreds of thousands of computers around the world, including the healthcare systems [12] [7]. It has exploited a vulnerability in the Windows operating systems, commonly known as EternalBlue. Once WannaCry is installed, it causes the encryption of the system and users' files. Hence, the locking of the medical ecosystem's files (e.g., patient's files, medical records, machines) [12], which leads to major disruptions in patient care and access to medical records.

2) Security vulnerabilities in the traceability of Medicines:

Fragmented supply chain: the pharmaceutical supply chain faces a major technical problem due to the multiplicity of the actors involved. The absence of a unified traceability system creates gaps in the tracking of medicines. This fragmentation has serious negative consequences, such as the increased risk of infiltration of counterfeit medicines into the supply chain. These counterfeit products represent a major threat to the public health, as they may be ineffective or even harmful [7][13].

Inefficiency of tracking: the current traceability mechanisms used by the healthcare ecosystem are often based on paper registers or centralized databases, and therefore they lack transparency and do not allow real-time tracking. This inefficiency leads to major difficulties when it comes to tracing the origin of medicines, particularly in the case of recalls or security incidents. The capacity to quickly and precisely track the origin and routing of medicines is crucial in order to guarantee patient security [14].

Outdated methods such as paperwork: the dependence on paper-based documentation within the healthcare ecosystem, particularly in the pharmaceutical supply chain, presents a significant risk of human error and falsification. Hence, these errors and manipulations can result in inaccurate information in the supply chain, compromising patients' security. Finally, paper documents can be easily modified and does not offer the level of security and reliability required in such a critical areas such as the healthcare and the pharmaceutical ecosystems [8].

As an example we cite the issue of counterfeit he fake anti-malarial medicines in Africa. In this context, the World Health Organization (WHO), exposed a series of difficult technical and regulatory issues [15]. Indeed, the counterfeiters use unregulated manufacturing facilities in order to produce

medicines of inferior, even of dangerous quality, often with incorrect ingredients or inappropriate doses of active substances. These products are then distributed through illicit networks, such as online sales on unregulated sites and parallel trade, which interfere with legal supply chains. This situation is in fact at the root of major weaknesses in the monitoring and quality control of medicines in many African countries, where regulatory systems sometimes lack resources, technical skills or adequate geographical coverage. The risks to public health are considerable, including therapeutic failures, resistance to medicines and direct damage to patients' health. Moreover, the detection and repression of these activities are extremely difficult as they require international cooperation and the use of advanced technologies to test and verify medicines, as well as a solid legal structure to track down the criminals. In addition to the health consequences, counterfeit medicines have an economic and social impact because they undermine confidence in the healthcare ecosystems and generate financial losses to the legitimate manufacturers, while also potentially financing other illegal activities [15].

3) Security vulnerabilities in the research and clinical trials:

Data manipulation: there is a significant risk of manipulating or tampering with clinical trial data to achieve biased or favorable results. This can lead to a distortion of research results, with the consequence of inaccurate and potentially dangerous conclusions [16].

Ineffective management of patients' consent: the ineffective management of patients' consent to the use of their data can lead to violations of patients' confidentiality and privacy. The consequences of such negligence are not only legal and ethical, but can also lead to a loss of public trust in medical research and healthcare institutions [17].

Data sharing: if the sharing of data between researchers is not accompanied by adequate security measures, then there is a security flaw as this can lead to data being exposed to the risk of leakage. This can be particularly worrying especially when the data are sensitive. Finally, breaching the confidentiality of patients taking part in clinical trials threatens the confidence in medical research [18].

As an example we cite the Research scandal at GlaxoSmithKline (GSK) in China (2013). It represents an emblematic case that has shaken confidence in pharmaceutical research practices. Investigators discovered several irregularities in the GSK clinical trials for cancer medicines. The main accusations concerned the manipulation of data in these trials, a very worrying issue in the medical field. This manipulation would have consisted in altering or omitting certain data to make the results of the trials more favorable or less risky, and thereby distorting the real efficacy and security of the tested medicines. This scandal has raised serious questions about the integrity of medicine research and approval processes in China and, by extension, around the world. The confidence of the public and healthcare professionals in the verification and approval processes for new medicines has been seriously undermined. Such acts of manipulation violate the ethical principles of clinical research, while compromising the security of patients who might use these medicines on the basis of the falsified data[1][2].

C. Securing healthcare applications with the blockchain technology

In this section, we present how the blockchain technology can contribute to address the nine security vulnerabilities presented in Section II-B. Table I summarizes the different measures discussed.

Addressing the use of centralized storage: the decentralized nature of blockchain technology eradicates the vulnerability of single point of failure commonly found in centralized storage systems. That is, medical records will no longer be stored on a central healthcare server, but rather will be distributed across a network of blockchain nodes. Each node will also hold a copy of the entire blockchain and this ensures the continued availability of data even if individual nodes are compromised or fail. This approach improves resilience in the face of cyberattacks and server failures, while enhancing the reliability of medical records management systems [7][12][19].

Addressing the insecure access: the use of cryptographic keys in blockchain technology offers a secure method of authenticating users and controlling access to medical records. Each user (patient or healthcare professional) has a unique key pair (public and private) that enables him/her to access data and verify his/hers identity without revealing any sensitive data, while offering an enhanced level of security. In addition, smart-contracts can automate authorization management on the basis of pre-established and specific rules, increasing the security and efficiency of healthcare data exchanges [7][20][21].

Addressing the lack of interoperability: blockchain technology facilitates interoperability between the different healthcare systems through the use of standardized protocols, so that healthcare information can be exchanged securely and transparently between several institutions, including hospitals, clinics and laboratories. The data stored on a blockchain follows in fact a standard format that guarantees the compatibility and readability between heterogeneous systems. This level of interoperability avoids the errors and gaps often associated with data transfer between heterogeneous systems, while preserving the confidentiality and security of patient data [7][22].

Addressing the fragmentation of supply chain issue: the traceability of medicines is greatly improved by recording each stage of the supply chain on the blockchain. From manufacturing to distribution, each transaction concerning a medicine is immutably and transparently recorded.

[1]https://ethicsunwrapped.utexas.edu/video/curbing-corruption-glaxosmithkline-in-china

[2]https://www.theguardian.com/business/2013/jul/15/glaxosmithkline-china-bribery-allegations

TABLE I: Addressing Security Vulnerabilities in Healthcare Applications using Blockchain Technology: A Summary

Vulnerabilities	Technical blockchain's solution/contribution
Use of centralized storage	**Data decentralization and replication**: blockchain technology solves this vulnerability by distributing data across multiple nodes and eliminating single points of failure.
Insecure access	**Cryptography and smart-contracts**: their use in blockchain technology enhances the control of access to medical records while offering a higher level of access security.
Lack of interoperability	**Standardized blockchain protocols**: blockchain technology uses standardized protocols to ensure fluid interoperability between the different healthcare institutions.
Fragmented supply chain	**Active tracking on the blockchain**: blockchain technology offers complete and transparent traceability of medicines, from manufacture to distribution, by reducing the risk of counterfeiting.
Inefficiency of tracking	**Real-time traceability**: the blockchain's real-time tracking capability (coupled with IoT sensors) enables precise tracking of medicines at each step of the supply chain.
Outdated methods	**Immutable digital records**: blockchain technology replaces paper documents with immutable digital records by reducing errors and the risk of forgery.
Data manipulation	**Immutability and transparency of records**: the immutability of blockchain technology guarantees the integrity of clinical trial data by preventing any manipulation.
Ineffective management of patients' consent	**Smart-Contracts for consent**: smart-contracts on blockchain technology can effectively and securely manage patient consent.
Data sharing	**Private and permissioned blockchains**: they enable secure, confidential data sharing between the research institutions.

This includes the origin of ingredients, manufacturing details, logistical information and arrival at pharmacies or healthcare institutions. This complete traceability helps to effectively prevent counterfeit medicines and to guarantee the quality and security of pharmaceutical products [23][24].

Addressing the tracking inefficacy: the integration of blockchain technology with technologies such as Internet of Things (IoT) enables precise, real-time tracking of medicines throughout the supply chain. IoT sensors can record data such as temperature, humidity and location of medicines and upload them directly to the blockchain. This approach ensures full traceability of medicines and enables the maintenance and verification of storage and transport conditions that are essential to the pharmaceutical quality. Thanks to this real-time traceability, healthcare actors can rapidly identify any potential problems such as temperature deviations or delivery delays, guaranteeing the integrity of medicines to their final destination [7] [25] [26].

Addressing the issues related to outdated methods: the blockchain technology effectively replaces paper documents with immutable digital records. In the healthcare ecosystem, all information and medical reports on clinical trial results are stored digitally on the blockchain. Each entry is timestamped and cryptographically linked to previous entries, forming an unalterable blockchain. This feature makes any falsification or unauthorized modification of the data impossible, while reinforcing the reliability and integrity of healthcare data [7][25].

Addressing data manipulation: the blockchain technology is particularly effective in helping to prevent data manipulation in clinical trials because the data are stored on the blockchain and protected from any modification. In addition, the use of smart-contracts can automate processes such as releasing funds and publishing results only after the validation of trial data. This transparency and immutability ensure that test results are reliable and credible [7][27][19].

Addressing the inefficiency of patients' consent management: the blockchain technology facilitates the secure and transparent management and recording of patients' consent using smart contracts. The latter can also be programmed to track patients' specific preferences regarding the use of their data, while ensuring compliant privacy management. Patients can modify or revoke their consent at any time and these changes are immediately recorded on the blockchain [28][29].

Addressing data sharing issues: private and permissioned blockchain networks offer a high level of security to guarantee data confidentiality, such as in clinical trials or research data sharing. In these networks, access is limited to authorized users and permissions can be accurately and flexibly managed, enabling the secure sharing of sensitive data. In addition, these networks can be configured to comply with specific healthcare regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) or the General Data Protection Regulation (GDPR) by guaranteeing regulatory compliance while taking advantage of the benefits of blockchain technology [7][30][31].

D. Overview of security concerns associated with blockchain technology

Blockchain technology is considered as a robust and secure data storage solution. However, it still vulnerable to some threats, as attackers are becoming increasingly ingenious at penetrating blockchain networks in order to obtain funds or interfere with normal operations. In this section, we provide an overview of the most common attacks on the blockchain (more details, on these and other attacks, can be found in [4][32]):

The 51% attack: it generally occurs in public blockchains using the Proof of Work (PoW) consensus mechanism when an attacker or group of attackers acquires more than 51% of the network's hash power. With this majority, they can influence the validation process of new blocks, cancel transactions by creating longer branches of the chain, or double-spend by confirming a transaction on the main chain and then canceling it on a chain they continue to develop in secret [33].

Sybil attack: it focuses on the creation of a large number of false identities by a single attacker in a decentralized network [34]. The attacker uses these identities to gain disproportionate influence over the network by potentially affecting consensus or reputation mechanisms such as manipulating votes for protocol changes, or engaging in behavior that degrades network trust and security, like fraudulently confirming invalid transactions or blocks [35].

Routing attack: it targets the blockchain's network infrastructure by intercepting or modifying data exchanged between network nodes. The attacker can use hacking methods such as Border Gateway Protocol (BGP) hijacking or Man-in-the-Middle (MITM) to intercept, modify or redirect blockchain data without the sending and receiving parties being aware of it. As a result, this attack can cause delays in block propagation, isolate certain network nodes or lead to the disclosure of sensitive information [36].

Double spending attack: in this attack, the same unit of digital currency is spent several times when an attacker successfully sends a transaction to one recipient and then quickly creates another transaction using the same funds but directed to another destination under his control. If the attacker can manipulate the network so that the second transaction is confirmed before the first, then he can successfully spend the same amount twice. This attack is particularly feasible for blockchains without robust double-spending prevention mechanisms, such as multi-node transaction confirmation [37].

Smart-contract vulnerabilities: these arise from coding or logic errors in smart-contracts deployed on the blockchain, such as poorly designed functions, data manipulation errors or unanticipated security flaws. Attackers can exploit these vulnerabilities to appropriate funds, manipulate contract behavior or disrupt automated processes. This includes attacks such as reentrancy (where one contract repetitively and maliciously calls another), overflowing or underflowing numbers, or exploiting function visibility [38].

E. Preventing blockchain-related security concerns in healthcare applications

In this section, we discuss the various prevention strategies that healthcare applications using blockchain can adopt to mitigate the prevalent attacks on blockchain technology, outlined in Section II-D.

Preventing 51% and sybil attacks: the use of permissioned blockchains can prevent 51% and sybil attacks. The prevention approach differs according to the type of application [39]:

- In medical records management, blockchain nodes are managed exclusively by accredited medical entities, such as recognized hospitals and healthcare organizations. These nodes are selected according to strict criteria of compliance with data security standards and computing capacity. The implementation of specific consensus mechanisms, such as Proof of Authority (PoA), improves security by limiting the creation of new blocks to trusted entities.
- In the traceability of medicines, the integration of nodes managed by pharmaceutical regulatory authorities ensures rigorous monitoring. Suitable consensus mechanisms could include variants of Proof of Stake (PoS) where the ability to validate transactions is proportional to the reputation or commitment of the regulating nodes.
- In research and clinical trials, there are nodes operated by recognized research institutions that guarantee data integrity and could use hybrid consensus systems. the latter could combine the validation of authorized entities with algorithmic mechanisms to detect and prevent any attempted takeover.

Preventing routing attack: communication channels must be secured to avoid routing attacks. The prevention approach differs according to the type of application [40]:

- In medical records management, Virtual Private Networks (VPNs) specifically designed for the secure transfer of medical data can be implemented. These VPNs use advanced encryption protocols such as TLS/SSL to ensure the confidentiality and integrity of data exchanged between hospitals and practitioners. In addition, the use of network segmentation techniques ensures that sensitive data are isolated and protected from unauthorized interception.
- In the traceability of medicines, secure channels need to be established between distributors and pharmacies, using end-to-end encryption technologies to ensure that medicines movement data are not intercepted or maliciously altered. Moreover, the implementation of asymmetric cryptography ensures that only authorized parties can access and verify the authenticity of traceability information.
- In research and clinical trials, the protection of data exchanged between the different parties involved requires a particular focus and the use of encryption protocols specific to this field of application can ensure the security of sensitive information.

Preventing double spending attack: in order to prevent double-spending attacks in healthcare applications, there are specific technical strategies to be implemented for each type of application [41]:

- In medical records management, the implementation of the PoA consensus protocol is crucial because only the authorized nodes of recognized healthcare entities can validate transactions. This method enhances the integrity of records by preventing duplication of entries. In addition, a layered verification system is implemented, where each transaction has to be validated by several authorized nodes, adding a further layer of security.
- In the traceability of medicines, multi-node validation mechanisms involve the participation of various actors in the pharmaceutical supply chain, such as manufacturers, distributors and pharmacies. Each transaction (e.g., the transfer of a batch of medication) must be validated by several of these entities by ensuring that the same unit of medication is not recorded more than once. Therefore, such a decentralized but coordinated approach effectively prevents attempts of double-counting in the system.
- In research and clinical trials, data integrity must be ensured where suitable consensus protocols are used, such as modified versions of Proof of Stake (PoS) or Proof of Elapsed Time (PoET), in which data validation relies on the reliability and seniority of the research institutions participating in the blockchain. This system ensures that clinical trial data (for example, test results or patient data) are not falsified or recorded incorrectly.

Preventing smart-contract vulnerabilities: the integration of regular security audits and penetration testing for smart-contracts helps to prevent smart-contract vulnerabilities [42][43]:

- In medical records management, regular security audits, particularly on compliance with healthcare data protection standards such as HIPAA, include in-depth penetration tests to detect potential security vulnerabilities. Moreover, continuous checks of smart-contracts can be performed to ensure that modifications or updates comply with patient data confidentiality standards.
- In the traceability of medicines, smart-contracts should be designed with built-in defense mechanisms against data manipulation and errors. They must also include cross-validation of transactions at each step in the supply chain and automated clauses to flag any inconsistencies. These contracts must be regularly audited for compliance with pharmaceutical regulations and for their ability to prevent unauthorized alteration of data.
- In research and clinical trials, smart-contracts integrate advanced security clauses to protect sensitive data. These clauses can include mechanisms for encrypting data at rest and in transit, as well as automated verification protocols to guarantee the integrity of collected data. Frequent audits must also be performed to guarantee that these contracts respect the strict ethical and regulatory standards of clinical research.

III. Discussions on the impact of blockchain in the healthcare sector

The implementation of blockchain technology in the healthcare sector promises to significantly transform the way healthcare data are managed by offering innovative solutions to improve security, transparency and efficiency. In this section, we discuss how blockchain technology is influencing and transforming the healthcare sector. We explore the changes it brings in terms of security and with regard to innovation in the healthcare applications discussed earlier.

A. Medical records management

In medical records management, blockchain technology is enabling a radical transformation in the way healthcare data are stored, shared and secured. It provides advanced solutions to the limitations of traditional systems in terms of data security, accessibility and integrity. As healthcare data will not be stored on a central server, but will be distributed across a network of nodes, this will increase its resistance to cyberattacks and server failures. Furthermore, blockchain allows the implementation of access control mechanisms based on tokens or cryptographic keys, enabling patients to control who can access their health data. These tokens or keys can be granted or revoked by patients, offering a higher level of consent and confidentiality. Indeed, the integration of smart-contracts in the medical records management allows to automate access to medical records, because they can be programmed to grant or restrict access according to predefined rules, improving the efficiency and security of data exchanges (see Section II-C).

Blockchain technology relies on cryptographic hash functions and signatures to ensure data integrity and immutability. Each data record on the blockchain is sealed with a unique cryptographic hash and any attempt to modify data would alter its hash, alerting the network to possible data corruption. In order to audit and track medical data over time, each transaction on the blockchain is timestamped, Offering an accurate and immutable record of when data was added.

In this context, the Massachusetts Institute of Technology (MIT) developed MedRec [44], an Ethereum-based prototype for medical records management. MedRec gives patients complete control over their health data and streamlines the communication between the different healthcare providers. The system uses smart-contracts to manage access authorizations, offering a transparent and secure solution for medical data exchanges. Similarily, Healthbank [45] represents another healthcare data management service that offers users a secure way to store, manage and share their medical information. Using blockchain technology, Healthbank ensures that patients' data remain under their complete control, while facilitating their use for personalized healthcare.

B. Traceability of medicines

The implementation of blockchain technology for the traceability of medicines offers an advanced technical solution, enhancing both the security and efficiency of the pharmaceutical supply chain [7]. The application of blockchain is crucial

in two main areas: (1) to address the issue of counterfeits and (2) to ensure transparency within the supply chain. To address the issue of counterfeits, each step in the medicine manufacturing and distribution process is recorded on the blockchain. This creates an unalterable history of each batch of medicines, from the production of raw materials to delivery to pharmacies or hospitals. In addition, medicines can be marked with unique identifiers such as Quick Response (QR) codes or Radio Frequency IDentification (RFID) tags, which will be then stored on the blockchain. When a medicine is scanned at any stage of its distribution, its authenticity can be instantly verified by consulting the blockchain. In this context, PharmaLedger [46] is a project supported by the European Union which uses blockchain to create a platform for verifying the authenticity of medicines, thereby reducing the risk of counterfeiting.

Regarding the supply chain transparency, blockchain technology enables authorized parties to track the progress of medicines in real time, from production to delivery. This transparency makes it possible to quickly detect any type of problem, such as late deliveries or temperature discrepancies during transport. Moreover, regulatory authorities can easily access blockchain data for audits and compliance checks, ensuring that all distributed medicines comply with quality and security standards. In this context, IBM Blockchain is working with various actors in the pharmaceutical industry to implement blockchain solutions that ensure complete traceability of medicines [47]. Their system enables medicines to be tracked from their point of origin to the consumer, guaranteeing that information about each medicine is accessible and transparent to all the involved parties [48].

C. Research and clinical trials

The integration of blockchain technology into medical research and clinical trials is revolutionizing the way research data are managed, as in the case of medical records management, while offering guarantees in terms of integrity and immutability. It ensures that once data have been recorded, they cannot be altered or deleted. This feature is fundamental to maintain the integrity of data collected during clinical trials. For example, test results, patient observations and biometric data can be stored securely, providing researchers with an indisputable source of truth. In addition, each transaction (or data record) is timestamped and recorded sequentially. This enables complete traceability and facilitates audits, ensuring that data have not been altered for the purpose of manipulating results.

Blockchain technology allows to record all steps in clinical trials, including initial protocols and any subsequent modifications. This is crucial for evaluating study integrity and ensuring that modifications are made in a transparent and justified manner. It also facilitates the transparent sharing of trial results, enabling researchers and stakeholders to access data in real time. This contributes to greater collaboration in the scientific community and accelerated medical discoveries.

In this context, ClinicalTrials.gov [49] represents a federal registry that explores the use of blockchain technology to record and track the different phases of clinical trials, ensuring data transparency and integrity. Another example is MediLedger [50] project uses blockchain technology to secure and track pharmaceutical data, including clinical trial information. MediLedger provides a framework where medicines and trial information can be securely shared between manufacturers, regulators and researchers [51].

IV. Conclusion

Blockchain technology is proving to be a valuable solution for solving security challenges, thanks to its unique features of decentralization, immutability and transparency. In this paper, we studied and identified the security vulnerabilities of three main classic healthcare applications (medical records management, traceability of medicines, and research and clinical trials). We then demonstrated how blockchain technology can effectively address these vulnerabilities. Later, we explored the most common attacks against blockchain technology and discussed suitable mitigation strategies for these attacks in the three main healthcare applications presented. Finally, we discussed how blockchain technology is impacting and transforming the healthcare sector.

References

[1] Jean-Paul A Yaacoub, Mohamad Noura, Hassan N Noura, Ola Salman, Elias Yaacoub, Raphaël Couturier, and Ali Chehab. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Generation Computer Systems, Elsevier*, 105:581–606, 2020.

[2] Abdul Razaque, Fathi Amsaad, Meer Jaro Khan, Salim Hariri, Shujing Chen, Chen Siting, and Xingchen Ji. Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain. *IEEE Access*, 7:168774–168797, 2019.

[3] Nour El Madhoun, Julien Hatin, and Emmanuel Bertin. A decision tree for building it applications. *Annals of Telecommunications*, 76(3):131–144, 2021.

[4] Shreshta Kaushik and Nour El Madhoun. Analysis of blockchain security: Classic attacks, cybercrime and penetration testing. *MobiSecServ 2023 (The Eighth International Conference On Mobile And Secure Services), IEEE*, 2023.

[5] Kevin Daimi, Ioanna Dionysiou, and Nour El Madhoun. *Principles and Practice of Blockchains*. Springer.

[6] Muhammad Anshari. Redefining electronic health records (ehr) and electronic medical records (emr) to promote patient empowerment. *IJID (International Journal on Informatics for Development)*, 8(1):35–39, 2019.

[7] Badis Hammi, Sherali Zeadally, and Jamel Nebhen. Security threats, countermeasures, and challenges of digital supply chains. *ACM Comput. Surv.*, 55(14s), 2023.

[8] Lorenz Trautmann, Tim Hübner, and Rainer Lasch. Blockchain concept to combat drug counterfeiting by increasing supply chain visibility. *International Journal of Logistics Research and Applications, Taylor & Francis*, pages 1–27, 2022.

[9] Aynaz Nourani, Haleh Ayatollahi, and Masoud S Dodaran. Clinical trial data management software: a review of the technical features. *Reviews on recent clinical trials, Bentham Science Publishers*, 14(3):160–172, 2019.

[10] Faheem Reegu, Salwani Mohd Daud, and Shadab Alam. Interoperability challenges in healthcare blockchain system-a systematic review. *Annals of the Romanian Society for Cell Biology*, pages 15487–15499, 2021.

[11] Kamalanathan Kandasamy, Sethuraman Srinivas, Krishnashree Achuthan, and Venkat P Rangan. Digital healthcare-cyberattacks in asian organizations: an analysis of vulnerabilities, risks, nist perspectives, and recommendations. *IEEE Access*, 10:12345–12364, 2022.

[12] Badis Hammi and Sherali Zeadally. Software supply-chain security: Issues and countermeasures. *Computer*, 56(7):54–66, 2023.

[13] Denise Blais. Strategies for preventing and mitigating counterfeit medication from entering the us supply chain. *Walden University*, 2022.

[14] Monalisa Sahoo, Sunil Samanta Singhar, and Sony Snigdha Sahoo. A blockchain based model to eliminate drug counterfeiting. *Machine Learning and Information Processing: Proceedings of ICMLIP 2019, Springer*, pages 213–222, 2020.

[15] NAFIU Aminu and MAHMUD SANI Gwarzo. The eminent threats of counterfeit drugs to quality health care delivery in africa: Updates on consequences and way forward. *Asian Journal of Pharmaceutical and Clinical Research*, 10(7):82–86, 2017.

[16] Aleena Banerji, Marc A Riedl, Jonathan A Bernstein, Marco Cicardi, Hilary J Longhurst, Bruce L Zuraw, Paula J Busse, John Anderson, Markus Magerl, Inmaculada Martinez-Saguer, et al. Effect of lanadelumab compared with placebo on prevention of hereditary angioedema attacks: a randomized clinical trial. *Jama, American Medical Association*, 320(20):2108–2121, 2018.

[17] Joyce Chen, Farnaz Farid, and Mohammad Polash. Federated learning: An alternative approach to improving medical data privacy and security. *Current and Future Trends in Health and Medical Informatics, Springer*, pages 277–297, 2023.

[18] Tonya White, Elisabet Blok, and Vince D Calhoun. Data sharing and privacy issues in neuroimaging research: Opportunities, obstacles, challenges, and monsters under the bed. *Human Brain Mapping, Wiley Online Library*, 43(1):278–291, 2022.

[19] Bessem Zaabar, Omar Cheikhrouhou, Faisal Jamil, Meryem Ammi, and Mohamed Abid. Healthblock: A secure blockchain-based healthcare data management system. *Computer Networks, Elsevier*, 200:108500, 2021.

[20] Randhir Kumar and Rakesh Tripathi. Secure healthcare framework using blockchain and public key cryptography. *Blockchain Cybersecurity, Trust and Privacy*, pages 185–202, 2020.

[21] Daniel Maldonado-Ruiz, Jenny Torres, Nour El Madhoun, and Mohamad Badra. Current trends in blockchain implementations on the paradigm of public key infrastructure: a survey. *IEEE Access*, 10:17641–17655, 2022.

[22] William J Gordon and Christian Catalini. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and structural biotechnology journal, Elsevier*, 16:224–230, 2018.

[23] Mueen Uddin. Blockchain medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *International Journal of Pharmaceutics, Elsevier*, 597:120235, 2021.

[24] Peng Zhu, Jian Hu, Yue Zhang, and Xiaotong Li. A blockchain based solution for medication anti-counterfeiting and traceability. *IEEE Access*, 8:184256–184272, 2020.

[25] Asad Ali Siyal, Aisha Zahid Junejo, Muhammad Zawish, Kainat Ahmed, Aiman Khalil, and Georgia Soursou. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography, MDPI*, 3(1):3, 2019.

[26] Elsi Ahmadieh and Nour El Madhoun. Artwork nfts for online trading and transaction cancellation. *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA), IEEE*, pages 235–239, 2023.

[27] Badis Hammi, Sherali Zeadally, and Alfredo J Perez. Non-fungible tokens: a review. *IEEE Internet of Things Magazine*, 6(1):46–50, 2023.

[28] Dara Tith, Joong-Sun Lee, Hiroyuki Suzuki, WMAB Wijesundara, Naoko Taira, Takashi Obi, and Nagaaki Ohyama. Patient consent management by a purpose-based consent model for electronic health record based on blockchain technology. *Healthcare Informatics Research, Korean Society of Medical Informatics*, 26(4):265–273, 2020.

[29] Prasanth Varma Kakarlapudi and Qusay H Mahmoud. A systematic review of blockchain for consent management. *Healthcare, MDPI*, 9(2):137, 2021.

[30] Luis B Elvas, Carlos Serrão, and Joao C Ferreira. Sharing health information using a blockchain. *HealthCare, MDPI*, 11(2):170, 2023.

[31] Tian-Fu Lee, I-Pin Chang, and Ting-Shun Kung. Blockchain-based healthcare information preservation using extended chaotic maps for hipaa privacy/security regulations. *Applied Sciences, MDPI*, 11(22):10576, 2021.

[32] Abhishek Guru, Bhabendu Kumar Mohanta, Hitesh Mohapatra, Fadi Al-Turjman, Chadi Altrjman, and Arvind Yadav. A survey on consensus protocols and attacks on blockchain technology. *Applied Sciences, MDPI*, 13(4):2604, 2023.

[33] Congcong Ye, Guoqiang Li, Hongming Cai, Yonggen Gu, and Akira Fukuda. Analysis of security in blockchain: Case study in 51%-attack detecting. *2018 5th International conference on dependable systems and their applications (DSA), IEEE*, pages 15–24, 2018.

[34] Badis Hammi, Yacine Mohamed Idir, Sherali Zeadally, Rida Khatoun, and Jamel Nebhen. Is it really easy to detect sybil attacks in c-its environments: a position paper. *IEEE Transactions on Intelligent Transportation Systems*, 23(10):18273–18287, 2022.

[35] Abdelatif Hafid, Abdelhakim Senhaji Hafid, and Mustapha Samih. A tractable probabilistic approach to analyze sybil attacks in sharding-based blockchain protocols. *IEEE Transactions on Emerging Topics in Computing*, 11(1):126–136, 2022.

[36] Raj Chaganti, Rajendra V Boppana, Vinayakumar Ravi, Kashif Munir, Mubarak Almutairi, Furqan Rustam, Ernesto Lee, and Imran Ashraf. A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges. *IEEE Access*, 2022.

[37] Afsana Begum, A Tareq, Mahmuda Sultana, M Sohel, T Rahman, and A Sarwar. Blockchain attacks analysis and a model to solve double spending attack. *International Journal of Machine Learning and Computing*, 10(2):352–357, 2020.

[38] Zulfiqar Ali Khan and Akbar Siami Namin. Ethereum smart contracts: Vulnerabilities and their classifications. *2020 IEEE International Conference on Big Data (Big Data), IEEE*, pages 1–10, 2020.

[39] Sarah Asiri and Ali Miri. A sybil resistant iot trust model using blockchains. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1017–1026, 2018.

[40] Mubashar Iqbal and Raimundas Matulevičius. Exploring sybil and double-spending risks in blockchain systems. *IEEE Access*, 9:76153–76177, 2021.

[41] Raifa Akkaoui, Xiaojun Hei, and Wenqing Cheng. Edgemedichain: A hybrid edge blockchain-based framework for health data exchange. *IEEE access*, 8:113467–113486, 2020.

[42] Sarwar Sayeed, Hector Marco-Gisbert, and Tom Caira. Smart contract: Attacks and protections. *IEEE Access*, 8:24416–24427, 2020.

[43] Jaturong Kongmanee, Phongphun Kijsanayothin, and Rattikorn Hewett. Securing smart contracts in blockchain. *2019 34th IEEE/ACM International Conference on Automated Software Engineering Workshop (ASEW), IEEE*, pages 69–76, 2019.

[44] Ariel Caitlyn Ekblaw. Medrec: blockchain for medical data access, permission management and trend analysis. *Massachusetts Institute of Technology*, 2017.

[45] Brígida Riso, Aaro Tupasela, Danya F Vears, Heike Felzmann, Julian Cockbain, Michele Loi, Nana CH Kongsholm, Silvia Zullo, and Vojin Rakic. Ethical sharing of health data in online platforms–which values should be considered? *Life sciences, society and policy, Springer*, 13:1–27, 2017.

[46] Yvonne Ziegler, Vincenzo Uli, and Jan Wortmann. Blockchain innovation in pharmaceutical use cases: Pharmaledger and mytigate. *Journal of Supply Chain Management, Logistics and Procurement, Henry Stewart Publications*, 3(4):312–325, 2021.

[47] Vance Morris, Rohit Adivi, Ratnakar Asara, Matthew Cousens, Nick Gupta, Nicholas Lincoln, Barry Mosakowski, Hong Wei Sun, et al. Developing a blockchain business network with hyperledger composer using the ibm blockchain platform starter plan. *IBM Redbooks*, 2018.

[48] R Bhuvana and PS Aithal. Blockchain based service: A case study on ibm blockchain services & hyperledger fabric. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 4(1):94–102, 2020.

[49] Daniel R Wong, Sanchita Bhattacharya, and Atul J Butte. Prototype of running clinical trials in an untrustworthy environment using blockchain. *Nature communications, Nature Publishing Group UK London*, 10(1):917, 2019.

[50] Jens Mattke, Axel Hund, Christian Maier, and Tim Weitzel. How an enterprise blockchain application in the us pharmaceuticals supply chain is saving lives. *MIS Quarterly Executive*, 18(4), 2019.

[51] Mary C Lacity, Rajiv Sabherwal, and Carsten Sørensen. Special issue editorial: Delivering business value throughenterprise blockchain applications. *MIS Q. Executive*, 18(4):3, 2019.