The challenges of using blockchain technology for medical data in public hospitals in Malaysia

Muhammad Izdihar Sahalan[1], Fathi Yusof[2], Hafiza Abas[3]

Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia,
54100 Kuala Lumpur, Malaysia

izdiharsahalan@gmail.com[1], fathi.kl@utm.my[2]
hafiza.kl@utm.my[3]

Article history

Received:
26 Oct 2023

Received in revised form:
10 Nov 2023

Accepted:
16 Nov 2023

Published online:
18 Dec 2023

*Corresponding author
izdiharsahalan@gmail.com

Abstract

The management and ownership of medical data will affect the future of decentralised healthcare data-sharing applications. Future research projects examining the use of blockchain technology to store medical data in governmental organisations in Malaysia will need to address governance concerns and consider how to regulate blockchain to achieve these objectives. This paper examines the present governance issues in the healthcare industry, identifies areas requiring further research, and outlines the most crucial factors for blockchain applications to function. This paper presents a systematic literature review that investigates the challenges associated with implementing blockchain applications for medical data in public hospitals in Malaysia. As a result of a systematic screening procedure, 53 primary studies were included in the final analysis, which discovered eleven significant issues individually. The analysis of eleven issues, including social, interoperability, and security concerns, presents significant challenges and solutions for blockchain applications for medical data. The systematic literature review provides insight into the current state of blockchain implementation in Malaysian public hospitals and offers helpful recommendations for addressing the identified challenges. Policymakers, hospital administrators, and blockchain technology developers can use these findings to create practices that facilitate the successful integration and implementation of blockchain applications in Malaysian public hospitals.

Keywords: blockchain applications, Malaysian public hospitals, medical data, personal data, systematic literature review

1. Introduction

Blockchain technology is unable to offer a comprehensive solution for all potential use cases [1]. Nevertheless, the primary objective of blockchain applications remains the utilisation of immutable and verifiable transaction records. Considering that a significant portion of the research is focused on "blockchain technology for medical data," it is imperative to establish a fundamental knowledge of the potential implications of blockchain technology for medical data, especially for public hospitals in Malaysia.

According to the Personal Data Protection Act (PDPA), medical data encompasses the process of storing, recording, and updating all health-related

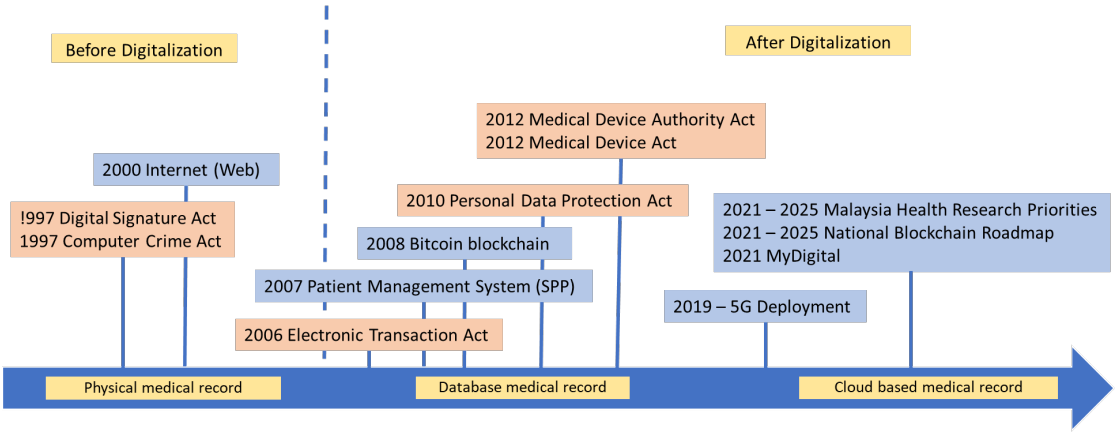
information on patients, regardless of whether it is obtained within a hospital setting or outside [2, 3]. The terms 'medical data' and 'medical record' are closely related in meaning, as defined in division 40, section 4 [4]. Medical data continues to be classified as "sensitive personal data" due to its nature as a personal information category falling under both "Personal data" and "Sensitive Personal Data," as defined in Act Division 1 Section 4 [4].

One example of a legal framework that provides support for medical data is the General Data Protection Regulation (GDPR), specifically in section 4(1). According to GDPR, any information that can be identified as an individual is considered medical data [5]. There exists empirical evidence that medical records, sometimes referred to as medical data, provide full details regarding a patient's medical background, diagnostic findings, test outcomes, and progression [6]. As a result, patient information is a complete set of medical records that resemble the legal connotations of medical data in PDPA and GDPR.

2. Related Works

Malaysian medical filing systems gradually adapting to the digitization of government cloud server databases [7]. The digitization efforts are collaborations between ministries such as the Ministry of Health (MOH) and the Malaysian Communications and Multimedia Commission (MCMC). The MOH has digital applications such as the Malaysian Health Reference Data Model (MyHRDM), Malaysian Health Data Warehouse (MyHDW), MyHealth portal, and MySejahtera apps. MyHDW is a central government server that stores all data for health data applications[8]. In addition, MySejahtera is one of the main public projects using blockchain to authenticate the COVID-19 vaccine certificate [9]. Malaysia prepared its goals to have a constructive nation with appropriate policies and guidelines for blockchain applications for public sector management [10]. The aim is to promote the nation's readiness to digitise the economy and expand the technologies used in the public sector [11, 12]. There an important medical data events in Malaysia that need to be highlighted before the digitalization era and after the digitalization era.

Figure 1. Highlighted events for the digitalization of medical data.



As illustrated in Figure 1, blockchain applications must comply with medical data regulations such as the PDPA issued by MCMC. In Malaysia, blockchain-specific

regulations are still limited to medical data, and the current legislative act pertains to medical services, contracts, and the digitalization of medical data.

2.1 Regulations

The study investigated the regulatory aspects of digitalization and contract management in the context of blockchain technology. The presence of blockchain technology has a resemblance to the previously described digitalization technology. The process of digitising data has emerged as an important reason for Malaysia's increased focus on formulating regulations on commercial transactions. Therefore, the enactment of the Personal Data Protection Act of 2010 (PDPA 2010) was undertaken to safeguard the integrity and confidentiality of economic transactions. In addition to the previous laws, there exist other statutes such as the Electronic Transactions Act of 2006, the Computer Crime Act of 1997, and the Digital Signature Act of 1997. Therefore, it can be observed that the regulatory framework surrounding blockchain technology is currently lacking, however, it is important to acknowledge that various domains such as digitalization, cybersecurity, and the Internet are impacted using blockchain technology.

Contract regulations are necessary to be highlighted to regulate smart contracts. The study shall need to highlight the equivalent elements mentioned in the Contracts Act (1950) [13]. Furthermore, another legal act related to contract are the Electronic Commerce Act (2006) which contain electronic contracts, including smart contracts, which qualify as digital signatures [14]. For it to assure the reliability and legitimacy of a contract, the application of a smart contract must align with the core values of common law [15]. Blockchain smart contracts are flexible and open to change based on the needs of an agreement, including the Contract Act (1950), which was enacted [14]. However, a study has indicated that blockchain smart contracts cannot be definitively referred to as legal instruments due to the inherent challenge in precisely translating the coded language of blockchain smart contracts into understandable human-spoken language [13]. The establishment of legislation and enactments regarding the use of smart contracts in Malaysia, particularly in the context of medical data and healthcare, needs a shift in direction [16].

2.2 Regulatory

According to the Securities Commission of Malaysia (SCM), the commissioner has recently declared a revised legislation related to cryptocurrencies, which is grounded in the Capital Market and Services Act (CMSA) of 2007. In the year 2019, SCM introduced a regulatory measure known as the Digital Currency and Digital Token Order, which was formulated under the regulations governing the capital market for cryptocurrencies. The previous rule pertains to the safeguarding of investments and encompasses the utilisation of digital currency and digital tokens. Furthermore, the Commissioner has formulated a distinct set of guidelines, known as the Digital Assets Guidelines, which cater specifically to investors involved in digital assets [17].

In 2016, the Central Bank of Malaysia (BNM) introduced a regulatory framework known as the Financial Technology Regulatory Sandbox Framework [16]. This framework was established to guide the regulation of various financial technologies, including cryptocurrencies and initial coin offering (ICO) initiatives, within the

Malaysian context [16]. BNM and SCM are working closely and collaboratively to develop policies and regulations for cryptocurrencies and digital assets, including ICO [19].

3. Blockchain applications use cases.

Blockchain use cases for healthcare medical data in public hospitals impact the capability of peer-to-peer (P2P) node transactions **[20]**. The node transmits data in the blockchain interconnected with the previous block storing encrypted data **[21]**. The device compatibility for blockchain, as mentioned by **Xiwei Xu, et al. [21]**, is that the blockchain can work with any device as long as the presence of the internet reaches the blockchain application. When the devices are connected, all the transaction events made are visible on the block explorer of the blockchain **[21]**.

There are several experiences of prototypes for the use of blockchain in hospitals from other countries. For example, in a scheme based on the blockchain as data storage, Luo, et al. [22] created an access control policy for blockchain data storage schemes. Also, Hussein, et al. [23] generated a security key with an integrated algorithm to access medical data from the blockchain data storage system. Again, more studies suggest using blockchain with different schemes and protocols for medical data, which include more discussion on blockchain applications in medical data in hospitals.

For the benefit of data-sharing in healthcare, some prototypes would allow researchers to evaluate the impact of guidelines on identical case studies in various countries, such as, for example, China[24-29], India[30, 31], Japan[32], the United States[33], Qatar[34] and Iran[35].

3.1 Malaysia blockchain applications

Examples of blockchain use cases for medical data in Malaysia are being researched, piloted, and listed below by author, title, issues, and provider. Table 1 shows ongoing blockchain research in Malaysia. A total of 16 studies from Malaysian institutions and universities have produced articles on blockchain in Malaysia, and there is still research ongoing.

Table 1. Blockchain applications in Malaysia

ID	Field	Provider
[13]	Legal (Smart Contract)	International Islamic University Malaysia (IIUM)
[36]	Application (Web Platform)	
[37]	Mobile Devices	Universiti Malaysia Pahang (UMP)
[38]	Healthcare system (Scalability)	Universiti Teknologi Malaysia (UTM)
[39]	Healthcare system (Medical Data Management)	
[40]	Healthcare system (Review)	KPJ Healthcare University College
[41]	Legal (Data Privacy law)	Universiti Tenaga Nasional (UNITEN)
[42]	Supply Chain	Universiti Tunku Abdul Rahman (UTAR)
[43]	Cryptocurrency	Universiti Malaya (UM)
[44]	Legal (Digital Regulatory)	

[45]	Cryptocurrency (Islamic Finance)	
[46]	Cryptocurrency (Digital Asset)	
[47]	Cryptocurrency (Islamic Finance)	Multimedia University
[48]	Cryptocurrency (Technology Adoption Behavioral)	Universiti Teknologi MARA (UiTM)
[49]	Cryptocurrency (Investment)	Universiti Sains Islam Malaysia (USIM)
[50]	Supply Chain (Food security)	Universiti Malaysia Sarawak (UMS)

Only nine out of sixteen studies experienced an impact on the blockchain application in Malaysia from a legal perspective (data, privacy laws, digital assets, digital regulatory, smart contract)[13, 41, 43, 44, 46] and non-legal (medical data administration, blockchain scalability, systematic review) [37-40]. There is still less appearance of the blockchain used for public health in Malaysia. However, some projects implement blockchain technology, such as the vaccine management system for Covid-19 [51].

4. Methodology

This review process includes three phases: (1) planning the research questions, (2) identifying and implementing the search strategy, and (3) mapping and presenting the results (shown in section 5). The phases of (3) can be observed in section 5. This approach facilitates the exploration of the research problem and enables a study to collect pertinent information from a variety of sources [52].

4.1 Planning the research questions

Determining the necessity of the research question is an essential task before conducting the review. The following research questions address issues related to the implementation of blockchain in the healthcare industry.

a. What are the major potential issues of applying blockchain technology for medical data in public hospitals in Malaysia?

Understanding the current issues in the public hospital system in Malaysia is important, and supports investigation into the research question (a). The need is to identify relevant articles from specific scientific databases that relate to the subject of medical data challenges. The selected articles encompass a wide range of themes. However, a systematic approach is employed to analyse and categorise these issues, to identify the most significant and related topics. Additionally, this method helps to identify areas where further research is needed.

b. What are the best practices for improvement relating to the use of blockchain technology for medical data in public hospitals in Malaysia?

The research question (b) aims to attain an understanding of the challenges and values necessary for forthcoming initiatives. Therefore, it is imperative to enhance the optimal recommendations for the government to establish well-defined guidelines for the implementation of blockchain technology to facilitate the exchange of public data within the public healthcare institutions of Malaysia.

4.2 Identify and conduct research strategy.

In extracting related articles, keywords were identified based on specific terms such as "blockchain," "medical data," and "policy." Then, all articles were selected and downloaded from the various sources journals and conferences from IEEE, ACM, ScienceDirect, and Emerald. The total number of articles searched resulted in 724 articles being screened at the first exclusion.

However, these outcome articles show that essential information on blockchain applications for medical data is missing. The identified criteria of the articles would then need to be screened by the quality and admissibility review, which is the research keyword and focus of the studies related to medical data.

The final review identified 53 articles to be included in the reference list. These articles were then summarised in an Excel spreadsheet and key questions were reviewed to understand the challenges and complexities of blockchain implementation in public hospitals.

5. Result and Discussion

In this section of the paper, the implications of the theory for looking into the challenges facing blockchain applications for medical data in general in Malaysia, the challenges facing blockchain applications for hospitals run by the government and other recommendations for various ways how Malaysian public hospitals might apply blockchain technology for medical data.

These potential issues of blockchain applications are categorized into subsections for medical data in public hospitals, the following section: access control, interoperability between hardware and software, cost, scalability, performance, energy, culture, security, privacy, and regulation. Each of the significant issues is identified as shown in Table 2.

Table 2. Category of issues

Issue	Challenges	Suggestions
Access Control	[22, 29, 53]	[23, 54-56]
Software	[22, 29, 37, 56, 57]	[34]
Hardware	[26, 53, 58]	[30]
Cost Maintenance	[27, 33, 59]	-
Culture	[53, 60-64]	[65, 66]
Scalability	[22, 24, 57, 60]	[27, 59, 67-69]
Performance	[2, 23, 24, 55, 57, 59, 70-72]	[24, 31, 73-75]
Energy	[53, 56, 59, 76]	[59]
Security	[59, 60, 77-79]	[54]
Privacy	[22, 29, 53, 56]	[32, 64, 70, 73, 80, 81]
Regulation	[30, 32, 33, 56, 67, 82]	[2, 22, 31, 53, 62, 82-84]

5.1 Challenges for blockchain applications for medical data

a. Access Control

Access control refers to the different levels of information access granted to various groups within a system [85]. The concern raised by Luo, et al. [22] is that medical data could be accessed by healthcare providers, online storage, and third-party researchers. Fan, et al. [29] highlighted the discrepancy between third-party technology and Article 17 of GDPR which seeks to protect personal data privacy. The most significant feature of blockchain technology is its ability to accurately confirm a transaction or event without losing any details [53]. This has enhanced researchers' and governments' confidence, as such illicit access to medical data without patient consent has been prevented [29]. Researchers are interested in using medical data to find solutions [29]. Additionally, Margheri, et al. [56] suggested that health centres should be given approval rights before they can access and approve medical data from medical devices. Qu [54], Sun, et al. [55], and Hussein, et al. [23] presented different blockchain system architectures. Qu [54] introduced a blockchain alliance chain for secure access to medical systems by health management departments, medical institutions, and patients. Sun et al. [55] presented a system that uses attribute-based encryption, blockchain technology, and the InterPlanetary File System (IPFS) storage platform for shopping and exchanging medical data. Hussein et al. [23] proposed using a private key to securely access medical data. This key is generated using a cryptographic hash-generating function, a genetic algorithm, and a discrete wavelet transform. The data is stored on a blockchain system [23].

b. Software

In software, interoperability refers to the ability of different components to work together seamlessly [86]. However, challenges related to software have been revealed in healthcare systems. The current healthcare systems have difficulty working with Blockchain, as noted by Luo, et al. [22] on different structures between centralized databases and decentralized linked blocks. Margheri, et al. [56] pointed out that the physical barriers of healthcare systems limit collaboration between centres. S and Farook [57] encountered obstacles when executing a smart contract on the Stellar blockchain due to the contract operations that cannot be changed. Despite the security of the application, Firdaus, et al. [37] warned against malware that can steal medical data through a root hack in the medical device operating system. According to Fan, et al. [29], the hospital system may have difficulties in transitioning to a blockchain application system since patients are required to maintain their virtual private keys to access their medical data, which can be lost or neglected. A model for software interoperability was suggested by Abdellatif, et al. [34], who proposed a model for software interoperability and a better blockchain configuration model, which includes edge computing.

c. Hardware

The studies listed show that hardware and infrastructure complexity makes it hard for systems to work together when changing to the blockchain system. Jeet and Singh Kang [53] discussed the complexity and expense issues of the blockchain technology devices that must complement present medical services. Li, et al. [26] observed that blockchain's complexity in the healthcare industry concerns security encryption adjustment. Połap, et al. [58] stated that blockchain devices must be equipped with a stable internet connection to safeguard encrypted private

data. Tripathi, et al. [30] demonstrate that Blockchain requires the assistance of IoT device automation and artificial intelligence to help maintain the Blockchain system's consensus mechanism.

d. Cost Maintenance

According to Zou, et al. [27], using a public blockchain to send medical data between hospitals costs a lot of money. The fees that are charged for Bitcoin public blockchains are based on cryptocurrency, and each transaction must have a fee as a payment for block mining [27]. Nevertheless, no funds have been set aside for medical institutions to pay fee incentives for using the public blockchain [27]. According to a study, hospitals still use separate health records instead of integrated health records because the situation makes it impossible for them to share data with other hospitals [33]. Additionally, Farouk, et al. [59] said that the number of people with expertise and experience in working with blockchain technology is limited and exorbitant. There appears to exist an option for hospitals to find a way near the high costs of maintenance and the lack of beginning incentives to implement blockchain applications [59].

e. Culture

The legal structure and healthcare adaptability must help hospital institutions adapt to blockchain applications [53, 61]. Jeet and Singh Kang [53] talked about how non-technologists might have trouble learning and getting used to the new blockchain-based hospital system because of cultural differences. The authors of Jeet and Singh Kang [53], and Yaeger, et al. [62] have talked about how to make medical records more accessible for older and disabled patients who can't use accurate biometric technology to get to them. Nevertheless, Li, et al. [60] said that making the older and disabled patients responsible for keeping their secret keys might indicate of loss of access and make it difficult for hospitals to share data. Some research [63], [53] and [64] identified cultural barriers to data exchange between healthcare facilities. Azaria et al. [33] said that the ineffectiveness and bureaucratic problems of the US governing system make it take longer for hospitals to share their medical data. Nanda and Nanda [65] said that professionals in different fields should learn about how to use blockchain in health data at universities and blockchain experts. Also, Jin, et al. [66] created a way to share medical data using blockchain and smart contract software with multi-authority attribute-based security to enhance the adaptability of blockchain applications. Concerns have been raised by Jin, et al. [66] and Jin and Xu [40] about how the current hospital system needs to work with more groups across the country or state to use blockchain applications to make health data secure [39]. For better health data security, Nanda and Nanda [39] said that research universities should be involved with hospital system innovations that can be used with blockchain applications.

f. Scalability

Scalability refers to the evaluation of the advantageous elements of a network, system, or process [87]. Blockchain transactions require a longer time than those

using Visa and other technologies, as pointed out by Wang, et al. [24] and Farouk, et al. [59]. Luo, et al. [22] highlight the problem of scalability with the huge amount of data, saying that there isn't enough room in the blockchain to store medical data like X-ray images. According to Li, et al. [60], the present hospital system used a centralised cloud storage by third parties which is not secure and there is a significant possibility that data will be leaked out and could be compromised. On the other hand, S and Farook [57] talked about the problems with using a permissioned blockchain that still needs central authority to gain access to the data. In this case, Li, et al. [60] highlighted that openness and control over who can see things still rely on the level of involvement the central authorities are in the whole system. Sharma, et al. [67] suggested that hospitals across the state or country should be able to share data safely and with access controls that respect people's privacy. Several studies also look at how scalable blockchain is right now [27, 59, 68, 69].

g. Performance

Numerous research have identified the challenges that hinder the performance of blockchain applications. According to Tandon, et al. [2], performance and efficiency require a proper installation for managing nodes and distributing private keys to patients. Sun, et al. [55] further stated that the speed of the internet is very important for performance when transferring data into the nodes. Wang, et al. [24] are concerned that the growing number of nodes will increase the latency of the blockchain to verify transactions. Uddin, et al. [70] state that the Bitcoin blockchain presents performance challenges that require a substantial amount of computational power for conducting both mining and authorization activities, particularly when integrating medical devices with sensors. S and Farook [57] also indicate that the Bitcoin public blockchain is an open and transparent system, but it is also insufficient and requires a lot of electricity. Concerns have been raised by Hirtan, et al. [71] about how adopting the right blockchain consensus mechanism might affect the way data is exchanged in blockchain applications. Liu and Tang [72] and Hussein et al. [23] also indicate appreciation for the differences in the consensus mechanism, including the effectiveness of the consensus mechanism in processing transactions. According to Hirtan, et al. [71], the speed of the internet does affect the use of blockchain applications in hospitals, since all blockchain nodes need to be able to access information for medical data to be properly transferred across the hospital's distributed network [71]. S and Farook [57] show that using smart contracts instead of the Bitcoin public blockchain to get data speeds things up by 15 TPS. As a result, it is more efficient to obtain data using Ethereum smart contracts [57]. Several studies have employed diverse blockchain elements to develop a prototype. Alsharif and Nabil [73] proposed a method to establish a worldwide marketplace for medical data by employing a secure system that relies on smart contracts integrated with Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) encryption, eliminating the need for trust. Farouk, et al. [59] proposed a medical system that utilises Ethereum smart contracts instead of the Bitcoin public blockchain. The choice was decided due Ethereum offers more efficient node management and critical distribution mechanisms, resulting in a faster transaction rate of 7 TPS (transactions per second) compared to

Bitcoin's 15 TPS. Several other studies [31, 74, 75] also look at the latency and speed of data transfer.

h. Energy

The Proof of Work (PoW) algorithm is the initial method used for Bitcoin mining [88]. According to De Vries (88), the annual power usage of PoW is similar to 7.67 gigawatts. It is comparable to the energy usage of countries such as Ireland (3.1 gigawatts) and Austria (8.2 gigawatts). Furthermore, Farouk, et al. [59] expressed worries about the rise of blockchain applications in the Bitcoin blockchain that could use a lot of power. Also, Jeet and Singh Kang [53] argue that adding blockchain to medical devices will need a lot of computer memory and power. Kuo et al. [61] and Margheri et al. [56] argue that a Bitcoin node network needs a lot of computer power which will affect the blockchain applications for hospital systems. Instead of PoW, there are consensus mechanisms that use less energy, such as Proof of Authority (PoA) or Proof of Stake (PoS), which were highlighted by Farouk, et al. [59]. These methods can be used with green energy sources like solar and wind power to lower the amount of electricity used [59]

i. Security

Concerns about data security have also been looked at in studies [60, 77-79], including data leaks, tampering, and data transfer from devices. Jeet and Singh Kang [53] believe that ensuring the security of the patient's private key is equivalent to ensuring the security of medical records. According to Farouk, et al. [59], PoW might be vulnerable to Denial of Services (DoS) attacks, based on where the technology's bottlenecks and single points of failure on the nodes are located. Also, Farouk, et al. [59] stated that an attacker who manipulates 51% of the PoW blockchain's computing resources can control the blockchain's transactions and conduct a double-spend attack. As Qu [54] studied it, the Practical Byzantine Fault Tolerance (PBFT) consensus method protects blockchain applications from the "51% attack" of changing data, keeping the system verification process. Furthermore, Jin and Xu [40] created a safe way for various organisations to share medical data by applying smart contracts on their blockchain applications.

j. Privacy

One of the privacy problems that have been talked about is the Blockchain's pseudonymous features. The existing data privacy legislation conflicts with the implementation of Blockchain technology in terms of patient's ability to exercise their right to remove their data according to Luo, et al [22]. Concerning sharing data with third-party services, Fan, et al. [29] mentioned the risk of setting medical data to the public, which might cause hospitals to encounter legal problems in the years to come. If medical data in the blockchain is incapable of being de-identified and protected, Jeet and Singh Kang [53] worry that it could be exposed to threats that compromise privacy. Concerns were also raised by Margheri, et al. [56] about threats like brute force attacks that could get to private medical data kept in the public blockchain network. It is not recommended by Margheri, et al. [56] to store sensitive data directly on the public Blockchain without initially de-identifying and encrypting the personal data. Additionally, Luo, et al. [22] concern the blockchain

immutable to be changed or removed because of the decentralized characteristics, implying that outdated and invalid data are unable to be deleted. Huang, et al. [64] suggest a system that can track data across all distributed systems in a way that is clear and complies with the rules of confidentiality. Alsharif and Nabil [73] and Huang, et al. [64] suggested a zk-SNARK encryption to safeguard and disguise the personal identification of medical data exchanges between patients and research organisations. Several privacy issues have also been looked at in research on data-sharing policies, protocols, and mechanisms [32, 64, 70, 80, 81].

k. Regulation

Several studies have shown that there are problems with regulations that affect the public and that need to be fixed for the benefit of legal best practices. A standard process and set of rules for regulation have been suggested by some studies [31, 82, 84, 89]. Concerning the implementation of blockchain technology in the present healthcare system, Margheri, et al. [56] cited legal ambiguities including the absence of codes of conduct (CoC). Aruna Sri and Lalitha Bhaskari [82] highlighted various terms used for medical data when describing the same subject, which could cause problems with how different hospital system store their medical data. Tripathi, et al. [30] highlighted the lack of standards and protocols for fair blockchain applications use, including data ownership and authorization. A study by Sharma, et al. [67] and Ding [32] indicated that blockchain security and privacy concerns are challenging for current hospital systems to trust and adjust to participate in the blockchain systems [32]. Another major challenge stated by Sharma, et al. [67] for patients concerned with using the blockchain system is the manipulation of personal information to be misused in cases for insurance claims, and job searches by particular individuals [67].

Jeet and Singh Kang [53] and Yaeger, et al [62], proposed that public bodies must tackle the administrative and regulatory challenges associated with blockchain applications. Luo, et al. [22] also emphasised the necessity of reinstating the enforcement of rules such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) in the United States. The implementation of these regulations is creating the conditions for an unprecedented clash between security and privacy violations, resulting in the decentralisation of medical data sharing [22]. Furthermore, Tandon, et al. [89] and Quaini [83] highlight the importance of concerns for policy maker and ministries to evaluate the potential benefits of blockchain technology by addressing specific concerns such as resources, technical performance and system requirements. Aruna Sri and Lalitha Bhaskari [82] suggested a way to settle terms disputes by suggesting a standardised and consistent structure for medical data. They suggested using the Proof-of-Word consensus method to make sure that the structure could be used by different systems to find and access data [82]. Kumar and Chand [31] examined MedHypChain, a regulatory protocol that utilises Hyperledger Fabric to monitor COVID-19 cases in a blockchain network, with a focus on patient-centric interoperability (PCI). Nevertheless, the approach put forth by [83] and [84] focusing on regulatory compliance and ethical norms for matters such as patient data ownership and access management was emphasised. Tandon, et al. [89] highlighted the importance of using a multidisciplinary strategy in research to tackle legal and ethical concerns

associated with compliance. Hence, Tandon, et al. [89] highlighted the need for international resolution for the implementation of blockchain applications.

6. Future Works

In addition to prototypes, survey analyses, and policy frameworks, the applications of blockchain technology in Malaysian public hospitals may be evaluated in several other ways. The research could generate valuable policy framework recommendations for each category of problem that can be resolved through a thorough legal evaluation of blockchain applications protecting medical data in Malaysian public institutions.

7. Conclusion

In the paper's discussion section, the implications of the open journal theory are examined concerning the use of blockchain technology for medical data in public hospitals, which generates implementation suggestions and challenges for public hospitals in Malaysia. The eleven issues are prospective research viewpoints for determining the impact of the legal implementation of blockchain technology on medical data. A prototype and theoretical framework based on selected studies could be used to analyse medical data from all possible perspectives to make policy recommendations and implement blockchain applications for public hospitals in Malaysia. In addition, each of these issues is a research gap with a unique concern that should serve as a guideline for public hospitals in Malaysia.

Based on the analysis issues, the most important points in the legal aspect for implementation of blockchain applications for public hospitals which is blockchain regulation, security, and node installation

a. Blockchain regulation issues

One that hinders legislative framework is the unavailable of a standard definition for this technology that comprises the element of privacy, smart contracts and track and trace regulations. For instance, the Malta Digital Innovation Act Authority (MDIAA) in 2018, acknowledges the legal definition and formal jurisdiction to assess various components of blockchain applications, including smart contracts, Distributed Ledger Technology (DLT), and nodes. The Maltese government has implemented legislation to authorise the appointment of authorities responsible for certifying various components of a company's blockchain application, including software, codes, computer protocols, and other architectural elements. These certifications are intended to verify the quality, features, traits, behaviours, and aspects of the applications.

b. Security issues

The security concerns represent a partially legal matter that is deliberated within the context of management considerations. These assessments also provide insights into the scope of technical innovation and data privacy under a new framework. The presented discussions serve as prime examples of the fundamental principle and

highlight the integration of the legal structure. According to Margheri, et al. [56], it is recommended to refrain from directly storing personal data on the blockchain while creating the medical data system. Thus, to address any legal uncertainties, it is imperative to establish precise regulatory guidelines for blockchain technology, including the formulation of codes of conduct (CoC) and the implementation of appropriate processes [56]. In their study, Huang, et al. [90] examined a security and safety system on the legal obligation of transferring ownership from a hospital to a patient.

c. Nodes installation issues

By engaging with blockchain applications, public hospitals are required to deploy blockchain nodes within their facilities to have access to the distributed ledger system of the blockchain. These nodes serve the purpose of verifying the veracity of medical data. The node can also be seen as a private node, such as a hospital, which is utilised for secure and confidential transactions following the parties' agreed-upon smart contracts. Based on the studies conducted by Wang, et al. [24], Margheri, et al. [56], Uddin, et al. [70], and Al-Marridi, et al. [74], it is recommended that the nodes involved in this context exhibit interoperability among the public hospitals. Additionally, these nodes should possess low latency capabilities and be supported by artificial intelligence automation, while also integrating with private blockchain applications.

These development needs to be implemented on new node infrastructure to ensure the stability of the node network [12]. The responsibility of specialists to ensure that medical data is handled with care and security should be considered in the discussion of public hospital guidelines [30]. Additionally, the cost of maintaining connections between devices that are required to operate across multiple hospitals needs to be considered [27]. By reviewing the entire public hospital system from a legal and non-legal perspective for medical data sharing between hospital-to-hospital operators, especially in the context of Malaysian public hospitals [33], all approaches and guidelines for blockchain applications can be adjusted to the culture of Malaysia.

In conclusion, these three crucial factors are identifying for the government to deal with action in regulation and implementations to widen the blockchain applications in healthcare industries.

Acknowledgement

This research was supported UTM Transdisciplinary Research Grant (PY/2018/03456).

References

[1] *Blockchain: background and policy issues*, 2018.
[2] A. Tandon, A. Dhir, A. K. M. N. Islam, and M. Mäntymäki, "[8] Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda," *Computers in Industry,* vol. 122, p. 103290, 2020/11/01/ 2020, doi: https://doi.org/10.1016/j.compind.2020.103290.
[3] *(ACT 709) PERSONAL DATA PROTECTION ACT 2010,* M. S. C. (MSC) 709, 2010.
[4] *Personal Data Protection Act 2010 (Act 709),* M. S. C. (MSC) 709, 2010.

[5] *Regulation (EU) 2016/679*, 2016.

[6] A. Bali, D. Bali, N. Iyer, and M. Iyer, "Management of medical records: facts and figures for surgeons," (in eng), *J Maxillofac Oral Surg,* vol. 10, no. 3, pp. 199-202, 2011, doi: 10.1007/s12663-011-0219-8.

[7] Kuala Lumpur Hospital and Putrajaya Hospital. "Medical Record." https://www.hpj.gov.my/portalv11/index.php/en/tutorials/medical-record (accessed.

[8] M. J. Fuller and D. M. K. S. Ahmad, *Malaysian Health Data Warehouse (MyHDW) 2015-2016 START UP: INITIATION*. Arkib Negara Malaysia: Ministry of Health, 2017.

[9] *Vaccine Management System (VMS) MySejahtera*, 2022.

[10] MOSTI, "National Blockchain Roadmap," 2022.

[11] M. PMO, "Dasar-dasar Kerajaan Malaysia - Wawasan Kemakmuran Bersama 2030," 2019. [Online]. Available: https://www.malaysia.gov.my/portal/content/30901?language=my.

[12] M. PMO, "MALAYSIA DIGITAL ECONOMY BLUEPRINT (MYDigital)," 2022.

[13] N. R. B. M. Zain, E. R. A. E. Ali, A. Abideen, and H. A. Rahman, "Smart Contract in Blockchain: An Exploration of Legal Framework in Malaysia," (in English), *Intellectual Discourse,* vol. 27, no. 2, pp. 595-617, 2019. [Online]. Available: <Go to ISI>://WOS:000504058000014.

[14] S. Associates, "Enforceability of Smart Contracts in Malaysia," 2022. [Online]. Available: https://www.lexology.com/library/detail.aspx?g=2f54dde8-5980-4aed-9159-86d6ac20eca6.

[15] *Contracts act 1950 (Act 136),* C. A. A. A. G. C. A. A. A. a. t. O. 2005), 1950.

[16] L. C. Yong. "Blockchain Law in Malaysia - Malaysian Legal Perspective." Ching Elaine & Co. https://www.lexology.com/library/detail.aspx?g=472d008e-f278-4cc3-9f76-d1598541a536 (accessed.

[17] SCM. "Digital Assets Guidelines Security Commision Malaysia." https://www.sc.com.my/regulation/guidelines/digital-assets (accessed.

[18] *Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Digital Currencies (Sector 6)*, 2018.

[19] *BNM and SC's Joint Response on "Policy confusion over cryptocurrencies"*, 2020.

[20] B. Portier. "Five considerations for blockchain applied to data privacy and GDPR." IBM. https://www.ibm.com/blogs/blockchain/2018/05/five-considerations-for-blockchain-applied-to-data-privacy-and-gdpr/ (accessed 25 November, 2020).

[21] Xiwei Xu, Ingo Weber, and Mark Staples, *Architecture for Blockchain Applications*. Springer Nature Switzerland AG 2019, 2019.

[22] Y. Luo, H. Jin, and P. Li, "[1] A Blockchain Future for Secure Clinical Data Sharing: A Position Paper," presented at the Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, Richardson, Texas, USA, 2019. [Online]. Available: https://doi-org.ezproxy.utm.my/10.1145/3309194.3309198.

[23] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. S. Tavares, and V. H. C. de Albuquerque, "[3] A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform," *Cognitive Systems Research,* vol. 52, pp. 1-11, 2018/12/01/ 2018, doi: https://doi.org/10.1016/j.cogsys.2018.05.004.

[24] Z. Wang, N. Luo, and P. Zhou, "[10] GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare," *J. Parallel Distrib. Comput.,* vol. 142, pp. 1-12, 2020/08/01/ 2020, doi: https://doi.org/10.1016/j.jpdc.2020.03.004.

[25] M. Wang, Y. Guo, C. Zhang, C. Wang, H. Huang, and X. Jia, "[33] MedShare: A Privacy-Preserving Medical Data Sharing System by Using Blockchain," *IEEE Transactions on Services Computing,* pp. 1-1, 2021, doi: 10.1109/TSC.2021.3114719.

[26] F. Li, K. Liu, L. Zhang, S. Huang, and Q. Wu, "[39] EHRChain: A Blockchain-based EHR System Using Attribute-Based and Homomorphic Cryptosystem," *IEEE Transactions on Services Computing,* pp. 1-1, 2021, doi: 10.1109/TSC.2021.3078119.

[27] R. Zou, X. Lv, and J. Zhao, "[21] SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system," *Information Processing & Management,* vol. 58, no. 4, p. 102604, 2021/07/01/ 2021, doi: https://doi.org/10.1016/j.ipm.2021.102604.

[28] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "[46] MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain," *IEEE Access,* Article vol. 5, pp. 14757-14767, 2017, Art no. 7990130, doi: 10.1109/ACCESS.2017.2730843.

[29] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "[50] MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain," *J. Med. Syst.,* vol. 42, no. 8, p. 136, 2018/06/21 2018, doi: 10.1007/s10916-018-0993-7.

[30] G. Tripathi, M. A. Ahad, and S. Paiva, "[12] S2HS- A blockchain based approach for smart healthcare system," *Healthcare,* vol. 8, no. 1, p. 100391, 2020/03/01/ 2020, doi: https://doi.org/10.1016/j.hjdsi.2019.100391.

[31] M. Kumar and S. Chand, "[20] MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic," *J. Netw. Comput. Appl.,* vol. 179, p. 102975, 2021/04/01/ 2021, doi: https://doi.org/10.1016/j.jnca.2021.102975.

[32] Y. Ding and H. Sato, "[41] Derepo: A Distributed Privacy-Preserving Data Repository with Decentralized Access Control for Smart Health," in *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 1-3 Aug. 2020 2020, pp. 29-35, doi: 10.1109/CSCloud-EdgeCom49738.2020.00015.

[33] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "[44] MedRec: Using Blockchain for Medical Data Access and Permission Management," in *2016 2nd International Conference on Open and Big Data (OBD)*, 22-24 Aug. 2016 2016, pp. 25-30, doi: 10.1109/OBD.2016.11. [Online]. Available: https://ieeexplore.ieee.org/document/7573685

[34] A. A. Abdellatif *et al.*, "[48] MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange," *IEEE Internet of Things Journal,* vol. 8, no. 21, pp. 15762-15775, 2021, doi: 10.1109/JIOT.2021.3052910.

[35] S. M. Pournaghi, M. Bayat, and Y. Farjami, "[49] MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," *J. Ambient Intell. Humaniz. Comput.,* pp. 1-29, 2020.

[36] M. Z. Bin Hussen and J. Bin Ibrahim, "New Business Model for Malaysian Ar Rahnu Using Blockchain as Sustainable Business," (in English), *Int Conf Inform Comm,* pp. 110-113, 2018, doi: 10.1109/Ict4m.2018.00029.

[37] A. Firdaus, N. B. Anuar, M. F. A. Razak, I. A. T. Hashem, S. Bachok, and A. K. Sangaiah, "[51] Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management," *J. Med. Syst.,* Article vol. 42, no. 6, 2018, Art no. 112, doi: 10.1007/s10916-018-0966-x.

[38] A. A. Mazlan, S. M. Daud, S. M. Sam, H. Abas, S. Z. A. Rasid, and M. F. Yusof, "Scalability Challenges in Healthcare Blockchain System—A Systematic Review," *IEEE Access,* vol. 8, pp. 23663-23673, 2020, doi: 10.1109/ACCESS.2020.2969230.

[39] Fariha Anjum Hira, Haliyana Khalid, Siti Zaleha Abdul Rasid, Shathees Baskaran, and Alam Md Moshiul, "Blockchain Technology Implementation for Medical Data Management in Malaysia: Potential, Need and Challenges," 2022, doi: 10.18421/TEM111-08.

[40] D. Elangovan *et al.*, "The Use of Blockchain Technology in the Health Care Sector: Systematic Review," (in English), *JMIR Med Inform,* Review vol. 10, no. 1, p. e17278, 2022, doi: 10.2196/17278.

[41] H. Baskaran, S. Yussof, F. A. Rahim, and A. A. Bakar, "Blockchain and the Personal Data Protection Act 2010 (PDPA) in Malaysia," in *2020 8th International Conference on Information Technology and Multimedia (ICIMU)*, 24-26 Aug. 2020 2020, pp. 189-193, doi: 10.1109/ICIMU49871.2020.9243493.

[42] J.-J. Hew, L.-W. Wong, G. W.-H. Tan, K.-B. Ooi, and B. Lin, "The blockchain-based Halal traceability systems: a hype or reality?," *Supply Chain Management: An International Journal,* vol. 25, no. 6, pp. 863-879, 2020, doi: 10.1108/SCM-01-2020-0044.

[43] Nur Husna Zakaria, Munir Abu Bakar, and Sherin Kunhibava, "Prospects and Challenges: Blockchain Space in Malaysia," *Malayan Law Journal Articles,* 2018.

[44] Mohammad Ershadul Karim and A. B. Munir, "Blockchain Technology: An Introduction in Malaysian Legal and Regulatory Landscape," *Malayan Law Journal Articles,* 2018.

[45] T. M. Sen, "Blockchain for Islamic Social Financing and Islamic Financial Institutions," *Malayan Law Journal Articles,* 2022.

[46] J. Rais, "Safeguarding Cryptocurrency and Digital Asset Investors in Malaysia," *Malayan Law Journal Articles,* 2022.

[47] M. R. b. R. Asfarina Kartika bt Shakri, "Gap Analysis on Islamic Fintech Laws Under the Islamic Financial Services Act 2013 of Malaysia: Issues and Recommendations," *Malayan Law Journal Articles,* 2021.

[48] N. F. Nazim, N. M. Razis, and M. F. M. Hatta, "Behavioural intention to adopt blockchain technology among bankers in islamic financial system: perspectives in Malaysia," *Romanian Journal of Information Technology and Automatic Control-Revista Romana De Informatica Si Automatica,* vol. 31, no. 1, pp. 11-28, 2021 2021, doi: 10.33436/v31i1y202101.

[49] A. Ayedh, A. Echchabi, M. Battour, and M. Omar, "Malaysian Muslim investors' behaviour towards the blockchain-based Bitcoin cryptocurrency market," (in English), *J Islamic Mark,* Mar 23 2020, doi: 10.1108/Jima-04-2019-0081.

[50] K. Y. Chan, J. Abdullah, and A. S. Khan, "A Framework for Traceable and Transparent Supply Chain Management for Agri-food Sector in Malaysia using Blockchain Technology," (in English), *Int J Adv Comput Sc,* vol. 10, no. 11, pp. 149-156, Nov 2019. [Online]. Available: <Go to ISI>://WOS:000504404900020.

[51] MySejahtera. "MySejahtera." https://mysejahtera.malaysia.gov.my/intro_en/ (accessed.

[52] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007.

[53] R. Jeet and S. Singh Kang, "[4] Investigating the progress of human e-healthcare systems with understanding the necessity of using emerging blockchain technology," *Materials Today: Proceedings,* 2020/11/19/ 2020, doi: https://doi.org/10.1016/j.matpr.2020.10.083.

[54] J. Qu, "[15] Blockchain in medical informatics," *J. Ind. Inf. Integr.,* p. 100258, 2021/08/01/ 2021, doi: https://doi.org/10.1016/j.jii.2021.100258.

[55] J. Sun, X. Yao, S. Wang, and Y. Wu, "[22] Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS," *IEEE Access,* vol. 8, pp. 59389-59401, 2020, doi: 10.1109/ACCESS.2020.2982964.

[56] A. Margheri, M. Masi, A. Miladi, V. Sassone, and J. Rosenzweig, "[5] Decentralised provenance for healthcare data," *International Journal of Medical Informatics,* vol. 141, p. 104197, 2020/09/01/ 2020, doi: https://doi.org/10.1016/j.ijmedinf.2020.104197.

[57] S. S and C. Farook, "[23] Blockchain & Machine learning Based Secure Personal Medical Record Storage and Sharing Platform - DataBlock," in *2019 4th International Conference on Information Technology Research (ICITR)*, 10-13 Dec. 2019 2019, pp. 1-6, doi: 10.1109/ICITR49409.2019.9407796.

[58] D. Połap, G. Srivastava, and K. Yu, "[18] Agent architecture of an intelligent medical system based on federated learning and blockchain technology," *J. Inf. Secur. Appl.,* vol. 58, p. 102748, 2021/05/01/ 2021, doi: https://doi.org/10.1016/j.jisa.2021.102748.

[59] A. Farouk, A. Alahmadi, S. Ghose, and A. Mashatan, "[9] Blockchain platform for industrial healthcare: Vision and future opportunities," *Comput. Commun.,* vol. 154, pp. 223-235, 2020/03/15/ 2020, doi: https://doi.org/10.1016/j.comcom.2020.02.058.

[60] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "[52] Blockchain-based data preservation system for medical data," *J. Med. Syst.,* vol. 42, no. 8, pp. 1-13, 2018.

[61] T.-T. Kuo, H. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association,* vol. 24, pp. 1211-1220, 11/01 2017, doi: 10.1093/jamia/ocx068.

[62] K. Yaeger, M. Martini, J. Rasouli, and A. Costa, "Emerging blockchain technology solutions for modern healthcare infrastructure," *Journal of Scientific Innovation in Medicine,* vol. 2, no. 1, 2019.

[63] S. Biswas, K. Sharif, F. Li, I. Alam, and S. Mohanty, "[28] DAAC: Digital Asset Access Control in a Unified Blockchain Based E-Health System," *IEEE Transactions on Big Data,* pp. 1-1, 2020, doi: 10.1109/TBDATA.2020.3037914.

[64] H. Huang, P. Zhu, F. Xiao, X. Sun, and Q. Huang, "[6] A blockchain-based scheme for privacy-preserving and secure sharing of medical data," *Computers & Security,* vol. 99, p. 102010, 2020/12/01/ 2020, doi: https://doi.org/10.1016/j.cose.2020.102010.

[65] S. Nanda and S. Nanda, "[43] Blockchain adoption in health market: a systems thinking and modelling approach," *J Asia Bus. Stud.,* vol. ahead-of-print, no. ahead-of-print, 2021, doi: 10.1108/JABS-11-2020-0457.

[66] H. Jin, C. Xu, Y. Luo, P. Li, Y. Cao, and J. Mathew, "[40] Toward Secure, Privacy-Preserving, and Interoperable Medical Data Sharing via Blockchain," in *2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS)*, 4-6 Dec. 2019 2019, pp. 852-861, doi: 10.1109/ICPADS47876.2019.00126.

[67] R. Sharma, C. Zhang, S. C. Wingreen, N. Kshetri, and A. Zahid, "[42] Design of Blockchain-based Precision Health-Care Using Soft Systems Methodology," *Industrial Management & Data Systems,* vol. 120, no. 3, pp. 608-632, 2020, doi: 10.1108/IMDS-07-2019-0401.

[68] V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. Burmester, "[38] A Hierarchical Multi Blockchain for Fine Grained Access to Medical Data," *IEEE Access,* vol. 8, pp. 134393-134412, 2020, doi: 10.1109/ACCESS.2020.3011201.

[69] S. Otoum, I. A. Ridhawi, and H. T. Mouftah, "[37] Preventing and Controlling Epidemics Through Blockchain-Assisted AI-Enabled Networks," *IEEE Network,* vol. 35, no. 3, pp. 34-41, 2021, doi: 10.1109/MNET.011.2000628.

[70] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "[11] Blockchain leveraged decentralized IoT eHealth framework," *Internet of Things,* vol. 9, p. 100159, 2020/03/01/ 2020, doi: https://doi.org/10.1016/j.iot.2020.100159.

[71] L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, "[24] Blockchain-Based Approach for e-Health Data Access Management with Privacy Protection," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 11-13 Sept. 2019 2019, pp. 1-7, doi: 10.1109/CAMAD.2019.8858469.

[72] S. Liu and H. Tang, "[2] A Consortium Medical Blockchain Data Storage and Sharing Model Based on IPFS," presented at the 2021 The 4th International Conference on Computers in Management and Business, Singapore, Singapore, 2021. [Online]. Available: https://doi-org.ezproxy.utm.my/10.1145/3450588.3450944.

[73] A. Alsharif and M. Nabil, "[29] A Blockchain-based Medical Data Marketplace with Trustless Fair Exchange and Access Control," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, 7-11 Dec. 2020 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9348192.

[74] A. Z. Al-Marridi, A. Mohamed, and A. Erbad, "[13] Reinforcement learning approaches for efficient and secure blockchain-powered smart health systems," *Computer Networks,* vol. 197, p. 108279, 2021/10/09/ 2021, doi: https://doi.org/10.1016/j.comnet.2021.108279.

[75] W. Wang *et al.*, "[16] A privacy protection scheme for telemedicine diagnosis based on double blockchain," *J. Inf. Secur. Appl.,* vol. 61, p. 102845, 2021/09/01/ 2021, doi: https://doi.org/10.1016/j.jisa.2021.102845.

[76] T. T. Kuo, "The anatomy of a distributed predictive modeling framework: online learning, blockchain network, and consensus algorithm," *JAMIA Open,* vol. 3, no. 2, pp. 201-208, Jul 2020, doi: 10.1093/jamiaopen/ooaa017.

[77] Y. Gao, H. Lin, Y. Chen, and Y. Liu, "[27] Blockchain and SGX-Enabled Edge-Computing-Empowered Secure IoMT Data Analysis," *IEEE Internet of Things Journal,* vol. 8, no. 21, pp. 15785-15795, 2021.

[78] S. Xu *et al.*, "[32] A Secure EMR Sharing System with Tamper Resistance and Expressive Access Control," *IEEE Transactions on Dependable and Secure Computing,* pp. 1-1, 2021, doi: 10.1109/TDSC.2021.3126532.

[79] X. Yang, T. Li, X. Pei, L. Wen, and C. Wang, "[47] Medical data sharing scheme based on attribute cryptosystem and blockchain technology," *IEEE Access,* vol. 8, pp. 45468-45476, 2020.

[80] J. Singh and K. Ghai, "[34] Security and Privacy Mechanisms for the New Generation Healthcare Applications Using Blockchain Technology," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 3-4 Sept. 2021 2021, pp. 1-6, doi: 10.1109/ICRITO51393.2021.9596107.

[81] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, and H. Lu, "[35] Towards Secure and Privacy-Preserving Data Sharing for COVID-19 Medical Records: A Blockchain-Empowered Approach," *IEEE Transactions on Network Science and Engineering,* pp. 1-1, 2021, doi: 10.1109/TNSE.2021.3101842.

[82] P. S. G. Aruna Sri and D. Lalitha Bhaskari, "[7] Blockchain technology for secure medical data sharing using consensus mechanism," *Materials Today: Proceedings,* 2020/11/02/ 2020, doi: https://doi.org/10.1016/j.matpr.2020.09.795.

[83] T. Quaini, A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "A Model for Blockchain-Based Distributed Electronic Health Records," *IADIS INTERNATIONAL JOURNAL ON WWW/INTERNET,* 2018.

[84] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," (in eng), *J Med Syst,* vol. 40, no. 10, p. 218, Oct 2016, doi: 10.1007/s10916-016-0574-6.

[85] R. S. Sandhu and P. Samarati, "Access control: principle and practice," *IEEE Communications Magazine,* vol. 32, no. 9, pp. 40-48, 1994, doi: 10.1109/35.312842.

[86] P. Wegner, "Interoperability," *ACM Computing Surveys (CSUR),* vol. 28, no. 1, pp. 285-287, 1996.

[87] A. B. Bondi, "Characteristics of scalability and their impact on performance," in *Proceedings of the 2nd international workshop on Software and performancep*, 2000, pp. 195-203.

[88] A. de Vries, "Bitcoin's Growing Energy Problem," *Joule,* vol. 2, no. 5, pp. 801-805, 2018/05/16/ 2018, doi: https://doi.org/10.1016/j.joule.2018.04.016.

[89] A. Tandon, P. Kaur, M. Mantymaki, and A. Dhir, "Blockchain applications in management: A bibliometric analysis and literature review," (in English), *Technological Forecasting and Social Change,* Review vol. 166, p. 19, May 2021, Art no. 120649, doi: 10.1016/j.techfore.2021.120649.

[90] H. Huang, X. Sun, F. Xiao, P. Zhu, and W. Wang, "[14] Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments," *J. Parallel Distrib. Comput.,* vol. 148, pp. 46-57, 2021/02/01/ 2021, doi: https://doi.org/10.1016/j.jpdc.2020.10.002.