Towards the Development of MetaMed: A Blockchain-based EHR System Integrated with a Browser-based Web Application for Interhospital Communication and Patient Data Ownership Empowerment

Mary Jane C. Samonte
School of Information Technology,
Mapúa University, Manila, Philippines
mjcsamonte@yahoo.com

Jim Daniel A. Giron, Ma. Michelle A. Pantoja, Angela Marie D. Tobias
School of Information Technology, Mapua University, Manila, Philippines
jdagiron@mymail.mapua.edu.ph, mmapantoja@mymail.mapua.edu.ph,
amdtobias@mymail.mapua.edu.ph

Abstract

Blockchain technology had developed to a level where it could serve the purposes of the healthcare sector. With EHR as one of the deliverables of E-Health, blockchain could be utilized to address issues regarding security, privacy, and interoperability. This warrants the need of a proposed system to serve as a basis to future implementations. This paper aims to rationalize the application of blockchain to the healthcare sector and deliver a proposed system for developing a blockchain-based EHR system with an integrated browser-based web application that effectively facilitates the transmission of electronic health records between authorized healthcare organizations and manages the viewership of anonymized patient data. By reviewing multiple literatures which are 35 in number, with the earliest publication on the year 2017, this study discusses the technological evolution of healthcare, the growing distrust on electronic health records, the components of blockchain, and considerations on the application of multiple blockchain model types to the healthcare sector, to rationalize the use of blockchain to the healthcare sector. Furthermore, based on findings of this study, a proposed system for developing a blockchain-based EHR system with an integrated browser-based web application that effectively facilitates the transmission of electronic health records between authorized healthcare organizations and manages the viewership of anonymized patient data is proposed.

Keywords
Blockchain, Healthcare, EHR, privacy and interoperability

1 Introduction
Blockchain technology is a shared, immutable ledger of all transactions across participating parties. It specializes in storing valuable data while ensuring its security and integrity. Thus, it makes business and organizational procedures of various industries more effective, legitimate, and secure. The characteristics of blockchain include immutability, decentralization, visibility, and traceability. Immutability can be defined as the ability of the blockchain ledger and the data to remain unaltered and unchanged from malicious tampering, while decentralization refers to having no central authority that controls the data without needing the service of a trusted third party. Meanwhile, visibility is where anyone in the network can view all blockchain transactions transparently, whereas traceability refers to the ability to trace the data with verifiable timestamps (Abu-Elezz et. al. 2020).

E-health is a unique healthcare environment built on technology to automate health-related fields. One of the fundamental components of e-health is electronic health records (EHRs), a documentation of patients' health records. And since blockchain technology stores valuable data from various industries like business and intelligent contracts (Abu-Elezz et. al. 2020), the healthcare sectors also benefit from the technology's characteristics. The application of blockchain in EHRs will help address the issues of security, privacy, and interoperability of data (Mayer et al. 2019).

Healthcare professionals need medical records to diagnose their patients effectively. Thus, Electronic Health Records (EHRs) were developed, an advanced collection of medical records that helps improve clinical outcomes' performance and reduces delays in treating patients. However, there are still issues that EHR systems must address, such as system security, identity theft, system failure, inaccurate information, and so on. Hence, blockchain can be used to improve the EHR system, according to Ayesha Shahnaz et al. (2019), because it has features that strengthen the privacy, security, confidentiality, and decentralization of medical records stored in EHR. Healthcare is a vital part of our daily life. When people visit hospitals or clinics for checkups and other operations, each individuals' activities performed in the hospitals or clinics are recorded. Medical data is an important resource for healthcare organizations and medical research, wherein the gathered data is used to improve quality care and increase efficiency and productivity (NEJM Catalyst 2018). Next, with the massive increase in the volume of medical data and the use of traditional storage systems in storing data, concerns regarding scalability are raised wherein traditional storage systems are being questioned in terms of security, privacy, and availability. As mentioned previously, blockchain allows for shared health record access and is not reliant on a single point of failure. In this effect, the potential of the blockchain's decentralized peer-to-peer network to replace the traditional storage systems exhibits viability.

Furthermore, with valuable data involved, robust security is a must. Healthcare organizations are required to keep and store health records on computers and other medical devices containing patient health information. However, without adequately implementing security measures to safeguard information on both hardware and software, it will be a point of interest for cybercriminals. Implementing blockchain technology in healthcare will ensure safe medical data storage and eliminate potential cybersecurity risks and threats.

1.1 Objectives
The influence of blockchain in numerous professional settings is growing and studies concerning the application of blockchain to the healthcare sector are constantly emerging. With this the paper aims to (1) rationalize the use of blockchain in the healthcare field and (2) deliver a proposed system for developing a blockchain-based EHR system with an integrated browser-based web application that effectively facilitates the transmission of electronic health records between authorized healthcare organizations and manages the viewership of anonymized patient data, based on 104 studies which were collected, with the earliest publishing date on the year 2017. This paper discusses the following: Healthcare 4.0, the growing distrust on electronic health records (EHRs), components of the blockchain, and types of blockchain models whereby discussions of blockchain are applied to the healthcare context.

2 Methodology
The databases where the studies were taken from are the following: ScienceDirect (https://www.sciencedirect.com/) IEEE Xplore Digital Library (https://www.ieee.org/), Taylor & Francis Online (https://www.tandfonline.com/), ACM Digital Library (https://dl.acm.org/), SpringerLink(https://link.springer.com/), MDPI (https://www.mdpi.com/), National Center for Biotechnology Information (https://www.ncbi.nlm.nih.gov/), American Accounting Association (https://meridian.allenpress.com/cia), and The New England Journal of Medicine (https://www.nejm.org/).

2.1 Data Collection
There was a total of 106 studies collected. 35 remain after the application of filters. Finally, 35 were selected to be used in this study. The number of selected studies from each website after the filtering and selection process are as follows: ScienceDirect = 12, IEEE Xplore Digital Library = 10, Taylor & Francis Online = 1, ACM Digital Library = 1, SpringerLink = 2, MDPI = 1, National Center for Biotechnology Information = 4, American Accounting Association = 1, and The New England Journal of Medicine = 1. In total that amounts to 33 and with the addition of the two references from direct documentations, totals to 35. A total of 99 references are accounted in the searched studies of the table 1 because there were several other sources which had a single reference that was eliminated after the filters were applied.

Table 1. Reference count for each database

Database of Researches	Searched Studies	Filtered Studies	Selected Studies
ScienceDirect	38	12	12
IEEE Xplore Digital Library	35	10	10
Taylor & Francis Online	1	1	1

Database of Researches	Searched Studies	Filtered Studies	Selected Studies
ACM Digital Library	8	3	1
SpringerLink	8	2	2
MDPI	2	1	1
National Center for Biotechnology Information	4	4	4
American Accounting Association	1	1	1
The New England Journal of Medicine	1	1	1

2.2 Data Analysis

The previously mentioned studies were selected in relation to the topic of the study and consideration of their publication being by February 2017 at the earliest. Furthermore, the studies are then filtered depending on their relevance to the study and the subjects to be expounded upon. These subjects are *Healthcare 4.0*, *Distrust on EHRs*, *Components of Blockchain*, and *Types of Blockchain (Table 2).* After the application of filters, the studies are then analyzed and their findings or results are compounded to provide a detailed discussion on the aforementioned subjects, highlighting subtopics and various issues or factors surrounding the subjects.

Table 2. Filtered Subjects

Subject	Description
Healthcare 4.0	Studies that discuss the real-time remote interconnections and cloud services featured in the networking scheme of the patient-centric structure of the healthcare 4.0 concept (Ahmad et al. 2022). Although healthcare 4.0 initially began by the year 2015 through the introduction of artificial intelligence to medical services, the required recency of citations, earliest February 2017, still applies to studies accepted through this factor.
Distrust on EHRs	Publications that discuss the drastic levels of distrust to the steadily growing use of electronic health records (EHR) in the provisions of health and clinical services or research (Savitz et al. 2020). These levels of distrust may be sourced from various sources such as data quality, transparency, transmission, and interoperability.
Components of Blockchain	Assessments for the impact which blockchain may deliver in terms of security and authenticity (Zarour et al. 2020). The mentioned specifications must not necessarily be directly addressed by the concepts or applications indicated in such assessments. Contributions to the factors of security and authenticity may be a general effect, byproduct, or a product to another desired result.
Types of Blockchain	Primary studies which address the benefits and./or threats of the application of blockchain to the healthcare sector. This excludes content from sources such as newspapers, magazines (physical or digital), or politically inclined origins (Abu-Elezz et. al. 2020).

3 Results and Discussions

This literature review aims to cover and discuss four topics which are the following: the history of healthcare evolution and the concept of healthcare 4.0, the growing distrust on electronic health records (EHRs) with regards to data quality and privacy, the components of blockchain and their holistic functions, and the assessment concerning the application of various blockchain types in the healthcare setting.

3.1 Healthcare 4.0

The transition from Healthcare 1.0 to Healthcare 4.0 share a lot of common features with the evolution of Industry 1.0 to Industry 4.0, where it started with simple medication to more complex and intelligent medical processes and treatments (Li et al. 2021). The table 3 shows the phases of the healthcare evolution and their focus.

Table 3. Evolution of Healthcare

Phase	Focus	Issues	References
Healthcare 1.0	• Basic patient-clinician encounter • Diagnosis and treatment	• Insufficient production of medicine, medical, supplies, and equipment.	Jingshan Li et al. (2021), Chiehfeng Chen (2020)
Healthcare 2.0	• Monitoring devices • Medical equipment and technology	• There was no patient care across units and departments of health care organizations.	Jingshan Li et al. (2021), Abhimanyu Ahuja (2019), Chiehfeng Chen (2020)
Healthcare 3.0	• Electronic Health Records (EHRs) • Computer networks • Telehealth and remote care	• Incapable of speedy computations and large data storage • Inability to easily access medical literature and medical records	Jingshan Li et al. (2021), Chiehfeng Chen (2020)
Healthcare 4.0	• Artificial Intelligence • IT solutions • Medical wearable devices • Smart and interconnected health care	• Security and privacy of EHRs	Jingshan Li et al. (2021), Jigna Hathaliya et al. (2020), Guilherme Tortorella et. al. (2021), Giuseppe Aceto et. al. (2020)

Healthcare 1.0 has been the phase of a basic patient-clinician encounter; this is where a patient visits a clinic to have checkups, get prescriptions and medical care from a clinician, and vice versa. This type of patient-clinician encounter has been the conventional way of health care practice throughout the years. It was Healthcare 2.0 that had a much larger effect than Healthcare 1.0 because of major development in health, life science, and biotechnology. MRIs, ultrasound, and CT scans were the new medical equipment and devices that have been invented and increasingly used in health care delivery, treatment, and monitoring (Ahuja et al. 2019). Health care 3.0 was the phase of the development of EHRs or EMRs, they are the compilations of all the patient's data into a unified and computerized data health record. Telehealth and remote care have become possible in this phase. Lastly, the fourth healthcare revolution has integrated and equipped IT solutions and medical wearable devices as part of the health care delivery processes, where it achieves smart health, connected care, and personalized medicine. It was then the emerging pervasive, smart, and interconnected health care that has led to the evolution from Healthcare 1.0 to Healthcare 4.0 (Li et al. 2021), (Hathaliya et al. 2020).

Healthcare 4.0 uses a wide range of possibilities for using Industry 4.0 technologies, such as cloud computing, Big Data, and Internet of Things (IoT), in revolutionizing eHealth and its whole ecosystem (Tortorella et al. 2021), (Aceto et al. 2020). Cloud computing in healthcare satisfies the IT needs of the healthcare sector to simplify eHealth processes and interactions. Moreover, it provides hassle-free scalability and flexibility to healthcare professionals, which in turn improves clinical outcomes and practice efficiencies. Big Data has been massively implied in healthcare 4.0 because of how it stores a large amount of data, analyzes information quickly, and identifies information patterns and connections. With the massive increase in the volume of medical data, there has come the advancement of technologies such as stream processing systems, and clinical information automation (e.g., Electronic Health Record (EHR), Electronic Medical Record (EMR), Personal Health Record (PHR)). Lastly, the Internet of Things (IoT) applications proved to be essential in reshaping smart and modern healthcare. Wearable devices bring multiple benefits for patients, healthcare professionals, hospitals, and even insurance companies because it supports real-time monitoring of parameters and at the same time decrease overall healthcare costs (Aceto et al. 2020).

Through the aforementioned technologies and their applications to Healthcare 4.0, it creates smart and interconnected healthcare. It also presents a new future of health care delivery especially if implemented to the ongoing COVID-19 situation in the medical field. Healthcare 4.0 can improve supply chain (e.g., remote monitoring, use of ERP, digital platforms for communication with suppliers on COVID-19 essentials), patient diagnosis (e.g., telehealth, remote care), patient treatment (e.g., real-time recording of patient’s EHR), and patient follow-up (e.g., secure patient data sharing systems) (Tortorella et al. 2021).

3.2 Distrust on EHRs

EHRs are the digital version of paper charts in hospitals or clinics, where the records focus on the patient's overall health from all healthcare sources. Also, it is built to be shared among stakeholders and across more than one organization, making it accessible to everyone, especially by the patients (Heart et. al 2017).

Even though hospitals use EHRs on the daily basis, the experience of healthcare professionals concerning privacy issues makes them not fully trust the system. Privacy on EHRs refers to the right of an individual to keep personal information about themselves from being disclosed, transferred, or shared by others. Disclosing patient health information without the consent of the individual can lead to a data breach. It is important to note that consent to access and share the health information of a patient must be protected and considered confidential (Keshta and Odeh 2021).

Electronic Health Records (EHRs) are primarily used for diagnosis, treatment, and billing purposes. It is vital to ensure that EHRs data are high in quality because the higher the data quality, the more it will produce an accurate, reliant, and consistent quality care and performance (Ahuja 2019; Jabbar et al. 2020). Issues with the quality of data (e.g., incompleteness, inconsistency, inaccuracy) can hugely affect decision-making processes and risk patient safety. Take for example the data gathered during the COVID-19 pandemic. Healthcare professionals and clinicians highly depend on EHRs to understand the virus and its potential impact on a person’s health (Table 4). However, if inaccuracies are found in EHR data, it could affect the way clinicians interpret the data and the way public health responds to the COVID-19 pandemic (Binkheder et al. 2021).

Table 4. Negative Effects in the EHR system

Action	Effects	References
Retention of Patient Data	Using EHRs in storing patient data for a specified time may invade one’s privacy and indirectly jeopardizes fundamental democratic processes, including government scrutiny, whistleblowing, and political organizing.	Tsipi Heart et al. (2017)
Storing Paper Health Record to Electronic Health Record	There are privacy concerns in shifting from paper to electronic records. Storing personal records in EHR are prone to a data breach, experience encryption blind spots, and data bottlenecks.	Ismail Keshta et al. (2021)
Storing data in Cloud Computing Storage	Cloud service providers usually implement security standards to ensure the cloud environment is safe. However, there is a common risk such as being prone to data leakage, data loss, DoS attack, etc.	Yazan Al-Issa et al. (2019)
Updating Patient Records in EHR	Inaccuracies in EHR data significantly impact the quality of care and patient safety. Inconsistency or inaccuracy might jeopardize patient treatment and result in risk effects.	Samar Binkheder et al. (2021)

3.3 Components of blockchain

There is a total of 8 blockchain components which are fundamentally responsible for successful transactions. These components are collectively taken from the study's references which includes articles and official documentation of legitimate blockchain platforms such as Hyperledger and IBM. The blockchain components and a brief description of their role and responsibilities are shown in table 5.

Table 5. Blockchain Components

Component	Description	References
Ledger	Previous and current state data storage which is maintained by each peer node present in the network.	Shubhani Aggarwal and Neeraj Kumar (2021), Hyperledger (2022)
Smart Contract	Programs which are installed in the ledgers of the blockchain. These programs execute automatically when certain terms and conditions are met.	Shubhani Aggarwal and Neeraj Kumar (2021), IBM (2022), Hyperledger (2022)
Peer Network	A blockchain network utilizes a peer-to-peer network to effectively share resources without the implementation of a third-party server.	Shubhani Aggarwal and Neeraj Kumar (2021), IBM (2022)
Membership	This component is mainly used for permissioned blockchain models. It is the component which authenticates, authorizes, and manages identities.	Shubhani Aggarwal and Neeraj Kumar (2021), IBM (2022), Hyperledger (2022)
Events	Notifications in the blockchain network are created by events. These notifications consist of any significant operation in the blockchain network.	Shubhani Aggarwal and Neeraj Kumar (2021)
System Management	Creating, changing, managing, and controlling other blockchain components is the primary responsibility of this component.	Shubhani Aggarwal and Neeraj Kumar (2021)
Wallet	A component which ensures the security and confidentiality of user credentials or identity.	Shubhani Aggarwal and Neeraj Kumar (2021)
Channels	To ensure that transactions remain private and known only to selected peers, this component allows for subnets to exist in the network.	IBM (2022), Hyperledger (2022)
System Integration	Not a component of the blockchain but it is responsible for the blockchain's integration to external applications through a two-way connection.	Shubhani Aggarwal and Neeraj Kumar (2021) IBM (2022)

3.4 Types of blockchain

There are several types of existing blockchain models. These types are namely: private, public, hybrid, permissioned, consortium, and decentralized application. There are various considerations for applying blockchain models to healthcare such as patient identity, data security, data monitoring, immutability, consensus, and value. These blockchain models are applied to the healthcare context and are evaluated accordingly to the analytic network process (ANP) structure which incorporates the previously mentioned metrics (Zarour et al. 2020).

Every previously mentioned blockchain model performs differently when applied to a healthcare context. Those performances rely heavily on the model's nature and its fundamental implementations. Such are then iteratively discussed below for each model (Table 6).

Table 6. Blockchain models

Model	Description	References
Private Blockchain	• Privileges to write and view to prevalidated individuals/organizations. • Implements a private network. • Could grant public users restricted read permissions. • System is governed by a central authority.	Morkunas et al. (2019) Zarour et al. (2020) Alhadhrami et al. (2017)
Public Blockchain	• All content and consensus involve every member. • Participants could amount to thousands. • High latency in data transmission. • Suffers from scalability and privacy.	Morkunas et al. (2019) Fekih and Lahami (2020) Syed et al. (2019)
Hybrid Blockchain	• Utilizes the benefits of both the public and private blockchain. • Versatile model which allows the utilization of both public and private networks.	Zarour et al. (2020) Cui et al. (2020) Jeon and Hong (2019)
Permissioned Blockchain	• Directly intended for business use. • Verified members validate transactions in the network. • Has several variants: private, hybrid, and consortium blockchain.	Helliar et al. (2020) Lui et al. (2019)
Consortium Blockchain	• Combines the concept of private and public blockchain models. • Has the privacy and efficiency of private blockchains. • Control is not bounded to a singular entity. • Incorporates multiple entities with comparable privileges as participants.	Bhuiyan et al. (2018) Zarour et al. (2020) Chen et al. (2021)
Decentralized Blockchain	• Applications which incorporate a blockchain or P2P database through multiple devices. • Beyond the influence of entities individually.	Wang et al. (2018)

Based on the study of Zarour (2020), it could be determined that the private blockchain model is the most effective model to be used for healthcare purposes under the criteria of patient identity, data security, data monitoring, immutability, consensus, and value. Provided that the features included in blockchain are decentralization, immutability, and security, a higher level of implementation in terms of security should be applied for the healthcare sector as it holds sensitive information about the health of others. This higher level of security implementation is brought by the private blockchain model as its participants are very limited to prevalidated members, eliminating the possibility of falsifying records from external actors and reducing the occurrences from internal actors. Furthermore, the participation of public users is bounded to restricted read permissions with malleable arbitrary regulations, allowing for a certain level of flexibility should access be provided to users such as patients.

4 Proposed system

The proposed system utilizes a consortium blockchain model. Although the study of Zarour (2020) concluded that the private blockchain model is the most effective blockchain model for the privacy and security of data in the healthcare sector, it was mentioned in the study of Liu, Wu, and Xu (2019) that the presence of a centralized agency which possesses control of the blockchain could reduce the credibility of the data in the blockchain. To this effect, a permissioned blockchain model such as a private blockchain model allows for privacy and a permissionless blockchain such as a public blockchain enables multiple entities to contribute to the verification of information in the blockchain which reinforces integrity and credibility. A hybrid blockchain model may be applied as it allows for the capability of a public blockchain network with the privacy offered by a private blockchain (Jeon and Hong 2019) however, if applied to the context of healthcare, it is considered a data breach if a patient's records are disclosed to others without their consent (Keshta and Odeh 2021), including other patients. Overall, the consortium blockchain model fits the requirements in the technical and practical aspects of healthcare. It allows for multiple healthcare organizations to participate in the network while allowing for restricted read permissions for public users (Bhuiyan et al. 2018).

Multiple layers exist within the proposed system with varying components serving as actors on each layer. The components included in the proposed system consists of the users and organizations involved in the blockchain network, an integrated browser-based web application, and an abstraction of the internal components and process flow of the blockchain network. The components included in the framework are the ordering system (consensus) (Figure 1), the peers and the peer network, the ledger, and an external state database. Some of which are considered to be vital components of a blockchain (Aggarwal and Kumar 2021; Hyperledger 2022). Several connections are observable in the framework. Apparent in the design is the interaction of all the various users of the blockchain to the integrated browser-based web application (Figure 2). This is to allow for these users or clients to interact with the blockchain through a high level of abstraction (Aggarwal and Kumar 2021), enabling transactions to be forwarded and queries to be processed without the requirements of a fundamental understanding to the blockchain.

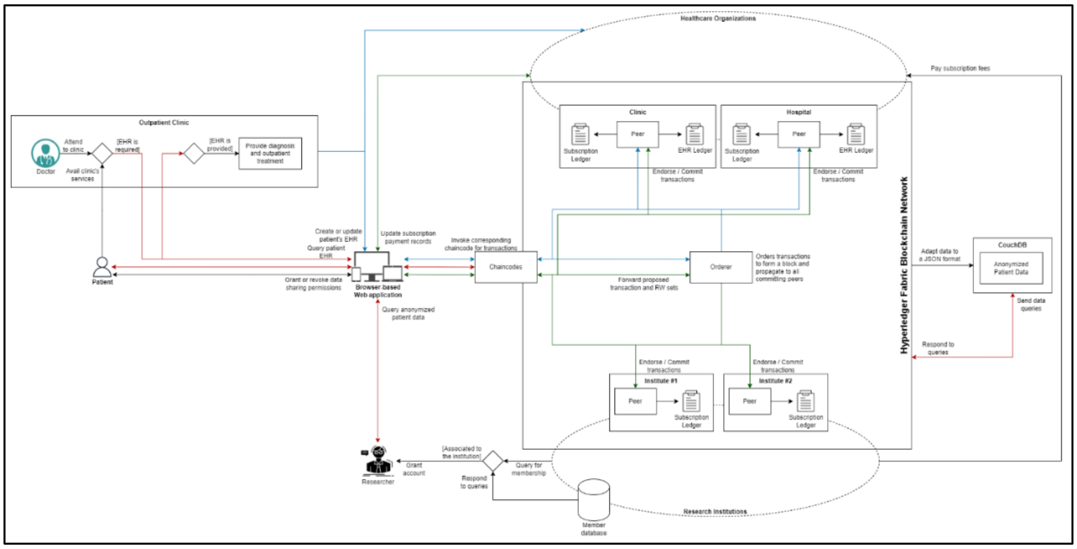

Figure 1. Proposed System

Legend:
- Data queries
- Record transactions
- Subscription transactions

Figure 2. Legend for Proposed System

With regards to the connection of the blockchain, it could be observed that only the "healthcare organizations" and "research institutions" have access to the ledgers as records are propagated. The separation of record type in this framework is abstracted and therefore does not illustrate the patient and financial record types available in the system (Figure 3). Regardless of such, patient records are only propagated to healthcare organizations, allowing multiple organizations to view patient data after obtaining authorization from the corresponding patient thus, preventing the occurrence of a security breach while retaining the integrity of patient data (Keshta and Odeh 2021; Binkheder 2021).

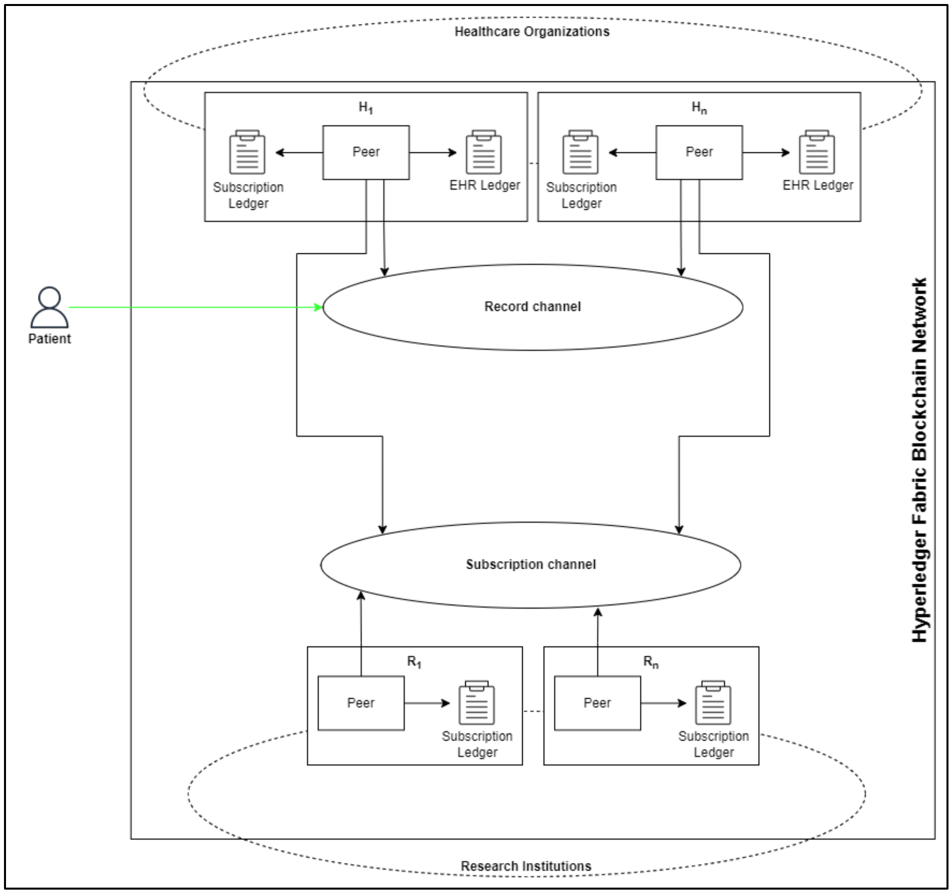

Figure 3. Underlying MSP and CA Mechanisms

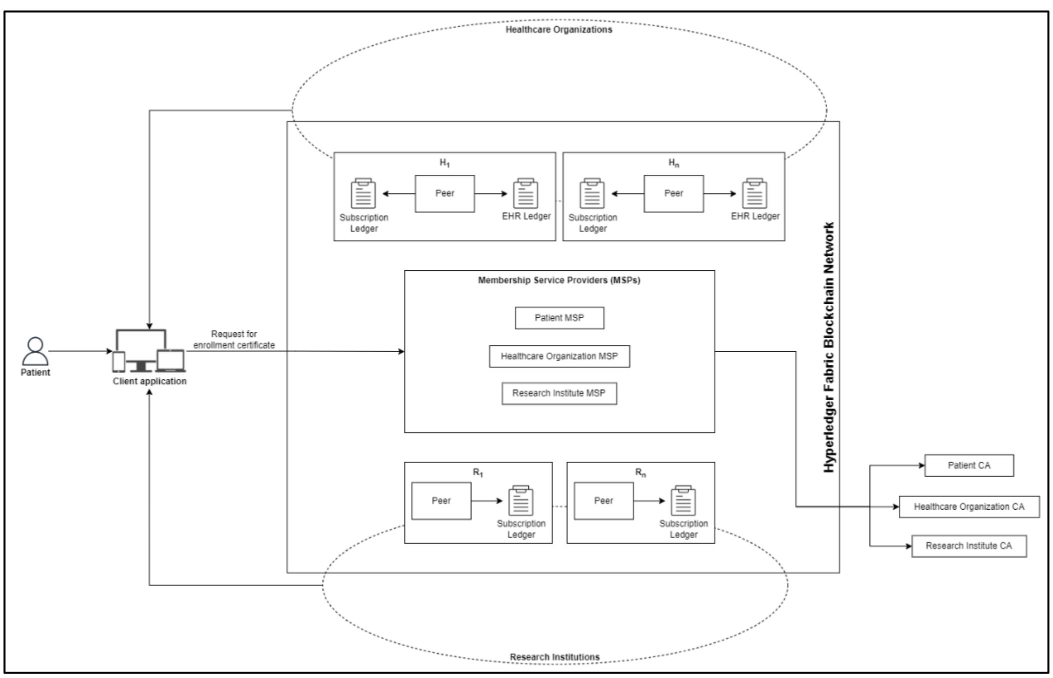

Figure 4. Proposed Blockchain Network Channel Design

For the implementation of this proposed system, the utilization of the Hyperledger Fabric framework is recommended because it primarily administers a consortium or private blockchain model (Figure 4). With the inclusion of this framework, additional components to the blockchain network are introduced. Their capabilities and application, whether they are directly applied, integrated, or developed, are provided in the table 7.

Table 7. Hyperledger Fabric Framework Components

Component	Capability	Application
Peer Nodes	• Comprises the peer network. • Hosts ledgers and smart contracts. • Responsible for executing chaincode, endorsing transactions, accessing ledger data, and interfaces with applications. • Fundamentally are servers or their respective devices.	Each healthcare organization in the system could be represented by a peer/s in the blockchain network and thereby has a copy of the records and participates in the consensus for transactions.
Organizatio ns	• Entities that participate in the network. • Could be represented by multiple peers. • Essentially collaborators in the network which act independently of each other. • Each has a recognized certificate authority provided by the Membership Service Provider (MSP).	Organizations are fundamentally represented in the blockchain network as the healthcare organizations involved.
Membership Service Provider (MSP)	• Oversees the creation of digital identities. • Propagates permissions to peers so they could be verified and participate in the network.	The Membership Service Provider or MSP serves to verify the identities of peers or healthcare organizations who are participating in the blockchain network.
Shared Ledger	• Keeps track of data status and history. • Consists of a database which holds current values and all the changes which led to the current values. • Current values are represented as the "world state" and the history is represented as the "blockchain".	Electronic Health Records could be placed in a single shared ledger to distribute through all participants in the blockchain network.
Chaincode	• Interchangeable to the term "smart contract". • Software which allows users to interact with the shared ledger. • State is exclusive to the invoked chaincode. • Could invoke other chaincode.	Chaincode could be developed to produce the varying interactions of the blockchain network which depends on user type. Facilitates the interaction between the healthcare organizations and the blockchain network.
Channel	• A subnet in the blockchain network. • Consists of two or more members. • Ensures that transactions are private and confidential to those who are not members of the channel. • Each member in a channel is authenticated and authorized before they could participate.	Several channels could be created as necessary. One channel may be created for all healthcare organizations to reliably transmit EHRs however, subgroups may also be created through the creation of more channels.
Clients	• End-user applications to propose transactions or changes to the blockchain network. • External components to the framework which are essential for all network operations.	Clients could be integrated through several interfaces such as web applications, mobile applications, etc. to read/write EHRs.
Ordering Service	• Organizes batches of transactions to a logical sequence to package into blocks.	The ordering system serves to communicate between peers.

Component	Capability	Application
	• Essentially the distributed consensus algorithm of the blockchain network. • A pluggable mechanism in the framework.	It is an internal component in the framework which adapts to its set configurations.

5 Implication and Conclusion

This literature review basically succeeded in rationalizing the application of blockchain to the healthcare sector and delivering a proposed system for developing a blockchain-based EHR system with an integrated browser-based web application that effectively facilitates the transmission of electronic health records between authorized healthcare organizations and manages the viewership of anonymized patient data. 104 studies were taken from various reliable sources which are then filtered to 35 studies and from the filtered studies, 35 studies were selected. A growing distrust has been developing with regards to the data quality and privacy of electronic health records (EHRs). Blockchain may be the solution to these concerns. Considering the technical requirements of healthcare, a private blockchain model is the most effective however, when practical requirements are imposed, a consortium blockchain model serves to provide the benefits of a private blockchain model while eliminating the existence of a central agency. The process and findings in this study could be used as a reference for papers which aims to apply blockchain technology to healthcare. The resulting system in this study could also be used as a basis for other frameworks concerning EHR transmission through the propagation of transactions in a blockchain network.

6 Limitation and future research

The limitations of the study are found in the focus of the study on rationalizing the application of blockchain to the healthcare sector. With the growing value of data, patients who at least have partial ownership of their own medical data should come to benefit from the financial gains incurred in its procurement and not intermediaries which obtained such data through various means. In this effect, the conceptual empowerment of patient data ownership was not covered through the exposure of the growing distrust on EHRs which is currently in the study. This study recommends future researchers to extensively discuss the value of medical data and its respective beneficiaries

Additionally, the study indicated a system which abstracts the intricacies of blockchain technology. Elaborations on such technology could become necessary for further studies. As such, the study recommends future research to provide a detailed layout of the various interactions between the internal and external components of a blockchain network.

References

Abu-Elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., and Abd-Alrazaq, A., Electronic health records in a Blockchain: A systematic review. Health Informatics Journal, 26(2), 1273-1288. DOI:https://doi.org/10.1177/1460458219866350, 2020.

Abu-Elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., and Abd-Alrazaq, A., The benefits and threats of blockchain technology in healthcare: A coping review. International Journal of Medical Informatics, 142, 104246. DOI:https://doi.org/10.1016/j.ijmedinf.2020.104246, 2020.

Aceto, G., Persico, V., & Pescapé, A., Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0. Journal of Industrial Information Integration, p. 100129. https://doi.org/10.1016/j.jii.2020.100129, 2020.

Aggarwal, S. and Kumar, N., Chapter Nineteen - Blockchain components and concepts☆☆Working model. Advances in Computers, Elsevier, vol. 121, pp. 387-398, ISSN 0065-2458, ISBN 9780128219911. DOI:https://doi.org/10.1016/bs.adcom.2020.08.019, 2021.

Ahmad, K. A. B., Khujamatov, H., Akhmedov, N., Bajuri, M. Y., Ahmad, M. N., and Ahmadian, A., Emerging Trends and Evolutions for Smart City Healthcare Systems, Sustainable Cities and Society, ISSN 2210-6707, DOI: https://doi.org/10.1016/j.scs.2022.103695, 2022.

Ahuja, A., The impact of artificial intelligence in medicine on the future role of the physician.PeerJ vol. 7 e7702. DOI:https://doi.org/10.7717/peerj.7702, 2019.

Al-Issa Y, Ottom MA, Tamrawi A., eHealth Cloud Security Challenges: A Survey. J Healthc Eng, doi: 10.1155/2019/7516035. PMID: 31565209; PMCID: PMC6745146.2019.

Alhadhrami, Z., Alghfeli, S., Alghfeli, M., Abedlla, J.A., and Shuaib, K., Introducing blockchains for healthcare, 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), pp. 1-4. DOI:https://doi.org/10.1109/ICECTA.2017.8252043, 2017.

Bhuiyan, M.Z., Zaman, A., Wang, T., Wang, G., Tao, H., & Hassan, M.M., Blockchain and Big Data to Transform the Healthcare. In Proceedings of the International Conference on Data Processing and Applications (ICDPA 2018). Association for Computing Machinery, New York, NY, USA, 62–68., 2018.

Binkheder, S., Asiri, M. A., Altowayan, K. W., Alshehri, T. M., Alzarie, M. F., Aldekhyyel, R. N., Almaghlouth, I. A., & Almulhem, J. A., Real-World Evidence of COVID-19 Patients' Data Quality in the Electronic Health Records. Healthcare 9(12) p. 1648. https://doi.org/10.3390/healthcare9121648, 2021.

Chen, C., Loh, E., Kuo, K., and Tam, K., The Times they Are a-Changin' – Healthcare 4.0 Is Coming!. J Med Syst 44, 40. https://doi.org/10.1007/s10916-019-1513-0. 2020.

Chen, M. Du, Q, Chen, J. and Ma, X., An Optimized Consortium Blockchain for Medical Information Sharing. IEEE Transactions on Engineering Management, vol. 68, no. 6, pp. 1677-1689. 2021

Cui, Z., Xue, F., Zhang, S., Cai, X., Cao, Y., Zhang, W., and Chen,J., A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN, IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 241-251. DOI:https://doi.org/10.1109/TSC.2020.2964537, 2020.

Fekih, R.B, and Lahami, M., Application of Blockchain Technology in Healthcare: A Comprehensive Study. In: Jmaiel M., Mokhtari M., Abdulrazak B., Aloulou H., Kallel S. (eds) The Impact of Digital Technologies on Public Health in Developed and Developing Countries. ICOST 2020. Lecture Notes in Computer Science, vol 12157. Springer, Cham. DOI:https://doi.org/10.1007/978-3-030-51517-1_23, 2020.

Hathaliya, J., and Tanwar, S., An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications 153, pp.311-335. https://doi.org/10.1016/j.comcom.2020.02.018, 2020.

Heart, T., Ben-Assuli, O., Shabtai, I., A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy. Health Policy and Technology 6, pp. 20-25. DOI:https://doi.org/10.1016/j.hlpt.2016.08.002, 2017

Helliar, C., Crawford, L., Rocca, L., Teodori, T., and Veneziani, M., Permissionless and permissioned blockchain diffusion, International Journal of Information Management, vol. 54, 102136, ISSN 0268-4012. DOI:https://doi.org/10.1016/j.ijinfomgt.2020.102136, 2020.

Hyperledger, Hyperledger Fabric Model. Retrieved February 15, 2022 from https://hyperledger-fabric.readthedocs.io/en/release-2.2/fabric_model.html. 2022.

IBM, Blockchain component overview. Retrieved February 15, 2022 from https://cloud.ibm.com/docs/blockchain?topic=blockchain-blockchain-component-overview, 2022

Jabbar, R., Fetais, N., Krichen, M., and Barkaoui, K., Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), pp. 310-317. DOI:https://doi.org/10.1109/ICIoT48696.2020.9089570, 2020.

Jeon, J. M., and Hong, C. S., A Study on Utilization of Hybrid Blockchain for Energy Sharing in Micro-Grid. 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 1-4, DOI:https://doi.org/10.23919/APNOMS.2019.8893033, 2019.

Keshta, I., and Odeh, A., Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), pp. 177-183. https://doi.org/10.1016/j.eij.2020.07.003., 2021

Lee, J., Chew, C., Liu, J., Chen, Y., and Tsai, K., Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract. Journal of Information Security and Applications 65, 103117. https://doi.org/10.1016/j.jisa.2022.103117, 2022.

Li, J., and Carayon, P., Health Care 4.0: A vision for smart and connected health care, IISE Transactions on Healthcare Systems Engineering, 11(3), 171-180. DOI: 10.1080/24725579.2021.1884627, 2021

Liu, M., Wu, K. and Xu, J., How Will Blockchain Technology Impact Auditing and Accounting: Permissionless versus Permissioned Blockchain. Current Issues in Auditing, 13 (2), A19–A29. DOI: https://doi.org/10.2308/ciia-52540, 2019

Mayer, A., da Costa, C., and Righi, R., Electronic health records in a Blockchain: A systematic review, Health Informatics Journal, 26(2), 1273-1288. DOI:https://doi.org/10.1177/1460458219866350, 2019.

Morkunas, V., Paschen, J., and Boon, E., How blockchain technologies impact your business model, Business Horizons, Volume 62, Issue 3, pp. 295-306, ISSN 0007-6813. DOI:https://doi.org/10.1016/j.bushor.2019.01.009, 2019.

NEJM Catalyst, Healthcare Big Data and the Promise of Value-Based Care, DOI:https://catalyst.nejm.org/doi/full/10.1056/CAT.18.0290, 2018.

Savitz S. T., Savitz L. A., Fleming N. S., Shah N. D., Go A. S., How much can we trust electronic health record data?, Healthcare, 8, 3, 100444, ISSN 2213-0764. DOI:https://doi.org/10.1016/j.hjdsi.2020.100444, 2020.

Shahnaz, A., Qamar, U., and Khalid, A., Using Blockchain for Electronic Health Records, in IEEE Access, vol. 7, pp. 147782-147795, doi: 10.1109/ACCESS.2019.2946373, 2019.

Silvestri, S., Esposito, A., Gargiulo, F., Sicuranza, M., Ciampi, M., and Pietro, G.D., A Big Data Architecture for the

Extraction and Analysis of EHR Data, 2019 IEEE World Congress on Services (SERVICES), pp. 283-288, DOI:https://doi.org/10.1109/SERVICES.2019.00082, 2019.

Syed, T. A., Alzahrani, A., Jan, S., Siddiqui, M. S., Nadeem, A., and Alghamdi, T., A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations, IEEE Access, vol. 7, pp. 176838-176869, 2019. DOI:https:/doi.org/10.1109/ACCESS.2019.2957660, 2019.

Tortorella, G. L., Fogliatto, F. S., Saurin, T. A., Tonetto, L. M., and McFarlane, D., Contributions of Healthcare 4.0 digital applications to the resilience of healthcare organizations during the COVID-19 outbreak. Technovation, p. 102379. https://doi.org/10.1016/j.technovation.2021.102379., 2021.

Wang, W. Cai, Z., Ernst, J. B., Hong, Z., Feng, C. and Leung, V. C. M., Decentralized Applications: The Blockchain-Empowered Software System. IEEE Access, vol. 6, pp. 53019-53033. DOI: https://doi.org/10.1109/ACCESS.2018.2870644, 2018.

Zarour, M., Ansari, M. T. J., Alenezi, M., Sarkar, A. K., Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records, IEEE Access, vol. 8, pp. 157959-157973. DOI:https://doi.org/10.1109/ACCESS.2020.3019829, 2020.

Biographies

Mary Jane C. Samonte has a double bachelor's degree in computer education and information technology. She also has two post graduate degree; Information Technology and Computer Science. She finished her Doctor in IT with a study focusing in Deep Learning. She has a wide range of research interests that are centered around educational technologies, gamification, mobile and ubiquitous learning, digital game-based learning, artificial intelligence in education, e-health, assistive technology, natural language processing, green computing and data analytics-based studies.

Jim Daniel A. Giron is a student in Mapua University – Makati who is currently working on his undergraduate degree under the program, Bachelor of Science in Information Technology, specializing in Enterprise Data Management.

Ma. Michelle A. Pantoja is a student in Mapua University – Makati who is currently working on her undergraduate degree under the program, Bachelor of Science in Information Technology, specializing in Cybersecurity.

Angela Marie D. Tobias is a student in Mapua University – Makati who is currently working on her undergraduate degree under the program, Bachelor of Science in Information Technology, specializing in Cybersecurity.