Blockchain for Healthcare Sector- Analytical Review

Nail Adeeb Ali Abdu¹ and Zhaoshun Wang²

¹,² Department of Computer Science and Technology, School of Computer and Communication Engineering, University of Science and Technology Beijing (USTB), Beijing 10083, China; zhswang@ustb.edu.cn

¹E-mail: b20190665@xs.ustb.edu.cn, n3a_alkershi@yahoo.com

Abstract. Blockchain is a collection of records and blocks that are integrated using cryptography. Every block consists of certain levels of cryptographic hash for the previous block in the form of a timestamp and the transaction data integral to the transaction record. The blockchain systems have currently used among the various set of industrial information networks. If effectively used, it shall help the system in having more secured levels of development. In this research review, the objective is to understand the gamut of blockchain implementation and to pursue the scope in the usage of the blockchain solutions in healthcare solutions. Review of the literature and data from the case scenario analysis throws light on a certain set of constraints and vulnerabilities of using the blockchain in healthcare which needs attention. Profoundly the constraints are about the quality of nodes verifying the blocks and the anomaly access of information from the blocks. By overcoming such constraints, there will be an improvement of effectiveness with which the system gets implemented.

Keywords: Cyber-attack, data Management, Blockchain, Healthcare, Personalized medicine, Gap Analysis.

1. Introduction

Information and communication technologies are evolving so rapidly that there is a paradigm shift in the way businesses function, the way transactions and sensitive information managed across the verticals. Among the contemporary range of solutions that have evolved in the ICT, blockchain is one of the new age developments, which increased the veracity and security of data management. The trend of increasing cyber-attacks on data and the prevailing information security concerns necessitate for a set of data security solutions in place, which makes a significant impact on the companies [1].

Information systems security has significant importance as any information breach might be a very challenging issue for many stakeholders associated with the system. For instance, in the case of the banking system or digital transactions, there are a distinct set of challenges[2]. Among the first set challenges, ensuring the data security and data integrity are predominantly important. In the case of the data security, it is about ensuring there is an appropriate kind of firewall systems,
anomaly detection systems etc. Whereas in the case of data integrity, it is profoundly about securing the data from any manipulation to the records and mitigating the risks of data security[3].

Blockchain, overall, can be defined as a system that ensures the transaction data is secured and monitored for amendments or trans positioning of data from one level to the other. Such system shall help the system in having more secured levels of development [1]. In this research proposal, the objective is to understand the gamut of blockchain implementation and to pursue the scope in the usage of the blockchain solutions in healthcare solutions.

In the further sections of this report, the emphasis is on the conceptual outline of the blockchain solutions and how the blockchain solutions used across industrial verticals. Further, it follows by a review of literature on the blockchain implementation in the healthcare industry. The further section discusses the gap in the existing system implementation and the potential scope for future research towards improvising contemporary solutions.

2.Blockchain System

Blockchain is a collection of records and blocks that are integrated using the cryptography. Every block consists of certain levels of cryptographic hash for the previous block in the form of a timestamp and the transaction data integral to the transaction record[3]. In terms of design, the blockchain can be more significant in terms of curtailing the chances for data or transaction input modification. It functions as a distributed ledger which can work on transaction records among the parties, making it efficient and effective, in terms of verification and holding the records in structured formats [4].

It is imperative from the literature that the blockchain is undeniably high levels of ingenious development. Today, across the verticals, the role of blockchain solutions is becoming an impeccable development. The crux of blockchain solutions is about the scope for disclosure of the transaction input public to the domain, but do not allow any changes to the transactions[5].

The blockchain model was introduced for cryptocurrency solutions initially. Over time the model of blockchain garnered the attention of other financial verticals, and today the blockchain solutions are more prevalent across a distinct set of industrial verticals [6].

Information managed on the blockchains exists as a shared and reconciled set of database. It supports the network with numerous benefits, as the blockchains are usually not stored in one single location and the data managed as truly public and verifiable by the stakeholders. As there is a lack of centralized versions for the information, it shall be very challenging for the hackers to corrupt the data. The other advantage is about how the blockchain is hosted across multiple computers in a similar instance, which makes it easier in terms of ease of access [7].

2.1 Instance of Blockchain

In a illustrative scenario, it can be stated that when there is need for documents to be reviewed and edited by the teams in an organization with in quick turnaround time, the traditional way of sharing the documents in collaborative networks like cloud or share point and the review in terms of modifications to the model has to undergo only at one source. Such structure is more prevalent in the databases of the banking and financial systems and other such verticals [5].
The way many cloud-based document or transaction systems exists in the current trend is supporting the organizations in having more effective improvisations, but the challenge exists when millions of records must be managed in terms of transaction records.

In the case of the transaction records, when there is too much of back and forth of data, it leads to time lag and redundancy in terms of records. But with the blockchain the authenticated review of the records can take place in real-time for the systems.

Some of the key reasons why the blockchain has gained significance in the domain are:

- The process is not owned by any single entity and it is profoundly decentralized.
- Cryptographic ways of managing the records are among the critical advantage in the system.
- Block chain is immutable and the scope in terms of tampering the data in the blockchain system is not feasible.
- Transparency in the system is very high and it shall help the organizations improve the overall solution outlook [4]

Management of the blockchain systems is predominantly handled by peer-to-peer network in the form of collection of nodes that are interconnected to the other. The nodes could be individual systems or the respective information systems that support in information exchange [7]. The blockchain system embraces the network of peer-to-peer network wherein the partitions in the entire workload is distributed among the participants, recognized as peers to the system. There is hardly any kind of central servers and the structure is formation of distributed and decentralized peers. Such system helps in improving the overall ways of information management and towards developing a comprehensive information network [6].

3.Blockchain Usage across Sectors

Blockchain solution mitigates the intervention of the intermediary inputs for the transactions. Personal computing has become an integral to the public usage by the respective stakeholders, by the interface created using the GUI, which is technically defined as wallet applications, which people shall use for the transactions. Transactions are usually connected by the processes of identity verification. It is pragmatic that the wallet apps shall transform into identity management solutions [8].

Though in the earlier days, the usage of the blockchain solutions was more prevalent in the cryptocurrency market, today, there is ongoing trends of embracing the blockchain kind of solutions to various industrial verticals. Categorically, in the banking, financial and insurance domain, the implementation of blockchain based transaction processing systems are yielding effective outcome, thus encouraging more other verticals to embrace the solution [9].

Some of the key areas wherein the blockchain solutions are vividly used are:

3.1 BFSI

Banking, finance and insurance industry is among the front runners in the adoption of block chain system, post its success in the cryptocurrency market. Considering the volume of transactions and
the intrinsic need for security and efficiency in information sharing among the groups, the usage of blockchain solutions in the BFSI domain has become significant and there are many companies that are experiencing the results of such integral usage [6].

3.2 Governance Systems
In many of the developed and developing countries, there are departments across the services, using the solutions like the blockchain. For instance, in the Indian government, there are many departments like the public works, judiciary department, land and infrastructure departments and many more are focusing on the usage of the blockchain solutions. Such holistic and integrated ways of developing an eco-system of information sharing shall support the organizations and stakeholders with more sustainable outcome [7].

3.3 Stock Trading
One of the critical areas wherein the role of blockchain solutions is considered significant in the stock trading domain. The potential in terms of adding the efficiency in share settlements turns to be strong use case for the blockchains in the trading industry [5]. The process of peer to peer trade confirmation models helps the parties in instantaneous settlements of the trade. Many intermediary processes like the clearing houses, custodians and the auditor’s role in the transaction processing is mitigated, thus enabling more quicker solutions in the transaction processing [10].

3.4 Supply Chain Auditing
Blockchain solutions usage in the case of the supply chain audits are turning to be potential developments which is improving the scope of reducing the pilferage or any scope for fault in delivery systems. With improved systems of instant sharing of information among the supply chain partners network, it becomes much easier for the organizations towards ensuring right kind of developments in the process [8].

3.5 Identity and KYC management
The other critical area wherein the blockchains solution is prevalently used is the identity and KYC management. For instance, the Know Your Customer records are very important and is essential across various service provider networks. When the system is integrated on the blockchain platforms, it becomes much easier for the system shareholders to have adequate and appropriate kind of information set, which will mitigate the risk of tampering the data and towards holistic improvement in the system [11].

3.6 Healthcare Systems
Blockchain systems usage in healthcare is one of the key developments that is turning to be more resourceful for the organizations. For instance, in the implementation of block chain model for managing the sensitive data of the patients and towards having easy access to updated and real-time information, it helps in quick access to patient data [2]. The medical professionals can have more significant information of patient’s health conditions and are able to plan the medical services in comprehensive manner.
4. Blockchain in Healthcare

Blockchain is gaining popularity in the healthcare industry as the age-old issues of the industry can be effectively addressed in the system implementation. Ineffective handling of the data, higher cost of data coordination among the stakeholders of the industry etc. are turning to be a challenging condition for the organizations. There are many healthcare companies eying on the blockchain solutions as a potential option towards addressing the limitations in the existing processes [3].

Key barrier in the healthcare system is about the data sharing and the transformation towards value-based care, wherein the critical role for the data sharing among stakeholders are very vital [12]. There is considerable level of silos in the current system for the companies and there is weaker section of information exchange among the groups and if the system is rightly integrated, it will help in connecting the silos and enabling optimum sharing and utilization of the resources, which can help in comprehensive development [6].

Interoperability is one of the critical issues for the healthcare industry. If the issue is addressed with effective integration and coordination among the stakeholders, it shall ease the process complexities and lead to more integrated approach in the system implementation [5].

**Figure 4.1.** Blockchain usage in various divisions of healthcare management [9].

There are vivid areas wherein the blockchain solutions in the healthcare can be potential solution. Few of the case dynamics that are imperative as per the literature are:

**4.1 Electronic Health Records**

One of the key areas wherein the solutions can be more robust for the organizations are the electronic health records solutions. In the case of the systems being in silos, the information of the patients is with different entities and in distinct formats. In the case of trauma care or emergency medical services, the scope of collating the distributed information towards historic information analysis of the patient becomes a challenge [8].

In a illustrative scenario, if the medical records of the patient are in different medical institution, and the current trauma care center needs access to such data or historic information of the earlier treatments to a patient, it might not be available, which turns to be a potential challenge [6]. But when there is integrated system, wherein the information is exchanged over the distributed...
ledger model, there is real-time access to the information, which can lead to sustainable kind of development process [13].

4.2 Third party information management
In addition to the medical professionals and the healthcare institutions, there are many third parties too who are integral to the healthcare industry. For instance, when the patient gets hurt in an accident and is admitted to trauma care center, there are certain records that are essential for the police department (or in certain instances the police might update information in their records about the cause of injury or other such kind of information) which might have significant impact on the conditions of treatment [6].

The other dimension is about the insurance companies processing the requests for insurance approvals and claims. If there is blockchain integrated data sharing system, there are potential ways in which the data could be more effectively managed among the systems [9].

In the presence of holistic system towards managing the blockchain solutions, there is imperative scope for instantaneous sharing of information among the stakeholders and the ones that could support in improving the kind of overall sustainable development model.

There are many case scenarios that are reviewed in the literature, pertaining to block chain-based healthcare system. Few organizations are currently engaged in and structured format of managing the block chain-based system for improving the healthcare for professionals and patients too. If the patient health history information is decentralized, it will lead to more comprehensive levels of service management. Right from health history tracking to claims management, fraudulent claims processing, classified information sharing for medical research, there are many areas in which the solutions can be more pragmatic [4].

A medical system developed on the Ethereum block chain as MedRec is a contemporary solution that prioritizes the patient record information to the agencies and enables transparent and accessible levels of view of medical data, thus making it simpler for the patients and doctors for purview. To ensure secured access to the data, the system works based on the Proof of Authority Mechanism.

4.3 Potential areas wherein Block Chain Solutions can be used
The blockchain solutions in the healthcare is currently used in the case of the medical records management, claims processing in the insurance for the healthcare, transaction records processing etc. Also, in many nations wherein the government schemes are prevalent for healthcare, towards managing the record of services to the patients, the blockchain based solution system can be more pragmatic.

As discussed above, there are phenomenal ways in which the blockchain based healthcare solutions can be more emphatic for potential healthcare services.

4.4 Integrated System of Patient Records
Longitudinal records of patients, with the structure of managing information like the episodes of treatment, disease registries, diagnostic report information, path lab reports, and the treatment
schedules can be combined from different sources into one system, in the blockchain environment. This kind of holistic information sharing and management among the key stakeholders shall support in quick response of treatment to the patient [9].

4.5 Master Patient Indices
Having a collaborated and one structure of data management shall ease the complexities of mismatch or redundancy in the data management, which shall support in improving the overall systems and practices that are integral to development.

4.6 Supply Chain Management
Among the healthcare companies, there is an integral system for robust supply chain process. If the patient data and the inventory data in the healthcare institutions are managed effectively with a blockchain solution, it will help in mitigating the pilferage and ensuring there is more systematic facets of handling the supply chain solutions [5].

4.7 Improving the Transparency and Security
Two of the critical factors in the healthcare data is about ensuring the security of the patient data and the other factor is about transparency in the system. In the case of the blockchain based models, the transparency and security can be realized if the right kind of system is embraced for implementation [8].

The Figure 4.2 below indicates the scope of how the blockchain systems are used in the healthcare domain and the key areas wherein the solution is highly used for operational processes.

![Figure 4.2](image)

**Figure 4.2.** Application of blockchain technology in healthcare [14].

5. Review of Literature

The work researched in the domain of blockchain implementation in healthcare. Profoundly the study is a review of the literature discussed in the earlier studies. The authors of the study indicate that there are distinct ways in which the research studies highlight the benefits and the cons of the system, but very few studies have focused on the live data conditions pertaining to how the block
chain in healthcare can work. But the authors reiterate the scope and efficacy of the system towards more emphatic levels of medical records management[15].

In [14], the authors the study too emphasize the need for more structured research in the domain, as predominantly many of the case studies discussed in the process indicates about the usage of the system. There are distinct set of conditions that requires the verification of the wallet application systems. Though there are prototypes and case scenario presentations, still in terms of creating significant system, there is need for better process and proven conditions for testing the application in healthcare domain[14].

In [16], the study has focused on the dimension of customization required for the healthcare systems. Depending on the conditions and the contextual implementation of the systems, the scope for sharing of the data in the healthcare systems might vary. It is paramount importance that such customization requirements are to be considered with the implementation of blockchain system[16].

The study highlights the fact that the blockchain system though creates complexities for hacking, still in terms of security, there are certain vulnerabilities and concerns that must be addressed in order to make it a potential and fool-proof system.

In [17], the authors of the study too have taken up the conditions of implementing the blockchain based system and has highlighted about five critical factors that make significant difference to the system implementation[17]. Firstly, the scope of digital access rules, followed by data aggregation, liquidity, identity management and the scope of data immutability. If the systems are effectively screened and customized for the aforementioned factors, there are potential chances that the system can be more robust and significant to the developments.

In [18], the focus of the study is about using the IT based framework structures that can support in integrated system implementation. The study discusses profoundly about the scope of using the IoT systems as a catalyst towards managing the transaction process and improve the process management quality of healthcare systems[18].

The authors of the study [19] has focused on the “Shared Nationwide Interoperability Roadmap” from the Office of the National Coordinator for Health Information Technology (ONC) and has evaluated the conditions that drive to the requirements of how the system has to be more robust and the models that are to be considered towards significant improvement to the systems. The study has discussed the crux factor of blockchain system, the decentralization as the structural framework that could be implemented as per the requirements that are to be addressed for the ONC system of managing the healthcare data[19].

Pseudonym Based Encryption with Different Authorities (PBE-DA) is proposed in [13], wherein PBE-DA will be resourceful for the patient anonymously to access, check or update their sensitive data on EHRs system. The system discusses more about the IoT kind of system integration that can support in improving the quality and access to the data for the organizations[13].

In [20], the study has focused on how effective the blockchain system could be in enabling the transition of the datacenter from institution centric to the patient data centric conditions. Highlighting certain set of limitations in the blockchain system implementation, the study triggers
the points towards understanding the key factors that can be integral to ensuring adequate and appropriate kind of system development[10].

In [20], the study highlights the scope of blockchain solution implementation towards understanding the developments in the domain and how effectively the model can be resourceful for implementing more integrated and transparent system in the biomedical and healthcare solutions[20], [9].

5.1 Blockchains in Personalized Medicine

Personalized medicine can be broadly defined as the classification of patients as a group based on indicators like genomic data, race, age, or gender and is an evolution of EHR/EMRs. Treatment, health plans and relevant advertising are developed based on classification as a group. Personalized medicine data faces a few issues from two aspects (i) ethical (ii) and access point of view [21], [22]. The ethical point of view raises concerns on individual data privacy and the family genome exposed which might not be desired by the entire family members. Further on access if the data is used for another study, it needs the patient/family consent on privacy aspect the approval of which might take the time or may turn away the patient/family from availing the healthcare. It might also lead to a case where the fear of data exposure might lead to false information supplied by the patient/family.

The integration of blockchain into the personalized medicine model may address the issues as mentioned earlier in data aspects. The feature of encryption will ensure that the private information is accessed by select few giving the patient/family confidence. Also, the record of access and notifications received will keep the patient/family informed. On the data end-user front, the doctors or researchers can access the data in a faster way reducing waiting time for approvals. This two-way seamless integration enables the patient/family to donate or sell their data for experiments or to other patients. The actual data stored in data lakes can be from clinical trials or clinical records but goes through authentication and decryption before final disclosure. The disclosure is limited to links to the data. These models can be perused in MedRec [23] and the Stony Brook Oncology project [24] and [25]. The pharmaceutical and insurance companies also can be end-users in these models.

5.2 Major Implementations

The idea to use blockchains in healthcare systems started in 2016. The use of blockchains for cryptocurrencies and the model of distributed ledger and better access control paved the way to replicate the model in healthcare systems. Few implementations described below:

Massachusetts Institute of Technology (MIT) developed a blockchain framework of healthcare system named MedRec [23]. The model focused on four aspects: data fragmentation, interoperability, patient focus, and medical diagnosis data.

Further it proposed contracts for managing data queries and linking between the patient and the caretaker. The drawbacks identified in this system are end-point security, flexibility, and patient intervention in the blockchain. The MedRec 2.0 [26] model in 2018 addressed patient inference from transactions and some scalability and privacy issues. But the end-point security remains a challenge.
In 2018 a model Medical Chain [27] was introduced with patient centricity in the management of EHRs. The key feature was the use of Hyper Ledger Fabric for access control. Along with access control to the patient the model provided a marketplace for negotiation with third parties for data access. MedTokens are introduced for patients to be purchased and stored. The drawbacks noticed were non-purchase of tokens and lack of legal qualification for MedToken security. Patientory [28] is a similar model like Medical Chain [27].

Along with tokens, the key aspect is privacy and security of patient are secured by HIPAA-compliant data storage systems. The tokens on this platform can be used for storage space or third party contract functions. In [29], [30] it is observed that privacy is an issue using blockchains Internet-of-Things (IoT) space. The user identities are observed to be inferred in the network despite encryption by monitoring device activity giving scope for attack by malicious users.

In [31], [30] the existing cloud-based healthcare systems are integrated with blockchains. [31] focused on a hypothesis of whether an existing cloud based EHR/EMR system could be built upon with improved data security with blockchains. The drawback observed in this model is complying to the privacy laws and regulations. In [30], the key focus is pseudonymity (username and password) and electronic contracts. The encryption method is called Elliptic Curve Cryptography resulting in a project named MediBChain. The drawbacks observed in this model is implementation costs, system migration and interoperability.

Healthcare Industry is witnessing one of the highest growths in revenues and volume of data by EHR/EMR. The is a growing need to store and share data among stakeholders for effective healthcare delivery in a secured manner. While the data is moving towards the cloud, there is a pressing need for its security which can be addressed by blockchain architecture. Few related works are described below.

In this [23] model, the framework enabled medical scientists, Government health authorities and healthcare stakeholders as end-users with data input from physician offices, hospital servers along with existing data storage infrastructure. Permission management is implemented with the decentralization of medical records by cryptography. Permission management firstly involves taking patients consent. The model works on smart contracts with a Proof-of-Work (POW) algorithm.

In this [32] model keeping the heterogeneous nature of healthcare data, a framework has been developed using blockchain and cloud technologies. Moving away from the centralization of data, the data is stored in a distributed environment ensuring better interoperability. Cryptographic techniques for user identity check is a pre-step before adding a new block on the existing chain for giving the requested data.

In this [33] model, a Blockchain Based Data Sharing (BBDS) framework is developed in a cloud environment. The users are verified and tracked for data requested in cryptographic techniques in a lightweight blockchain system. The system is divided into user, system management and storage layers. The user layer is for blockchain miners; the system management is for secure cryptographic authentication and storage layer is the data stored on the cloud for future uses. Further research on this work as indicated by the researchers, is communication and the authentication protocols in this framework.
A system in [34], is named MeDShare for healthcare data and uses a four-layer model. The key focus is monitoring the end-user for preventing malicious activities. The layers are user, data query, data provenance and structuring, and existing database infrastructure. The user layer is for actual research end-users, the data query layer is subdivided into querying that manages the data requests and trigger for mediation between blockchain and live environment, the data provenance and structuring layer is subdivided for authentication, processing, smart contracts, smart contracts database. The final data layer is that of the existing data.

This [24] model is developed on health information of cancer patients. The system is a membership service for healthcare data storage, multiple nodes, and application programming interfaces (APIs). The user verification a pre-step before access to data for blockchain miners. The database is stored on two locations local server and the cloud. The local server stores the patient cancer data, and the cloud organized categorical data. The access control is defined by patients with encryption based on symmetric key pair for each patient. The system performance is measured on privacy, security, and scalability.

This [31] model is designed keeping the patient as the end-user who desire to store their data on the blockchain. The blocks are added with the addition of a new patient with a timestamp. The verification of blocks happens cryptographically and contain the hash info of previous blocks. The advantages of the model indicated by the authors are avoiding single point of failure, patients right to access, ease of access to healthcare data and identification of malicious activity.

This model [35] is based on three layers, namely data sender layer, registration unit and private accessible unit. This model ensures the anonymity of patient data in its cryptographic mechanism. The data sender layer is accessed by patients to input all the data and store it cryptographically by checking the authenticity through the data receiver layer. The registration unit ensures the storage of credentials like username, password, and biometric details of the actual end-users. Private accessible unit is the mediator to regulate the flow of data in a secured channel to the end-user.

In this [36] model a mobile application and wearable devices are synchronized in a tree-based and batching approaches to address performance. The system is user-centric and has six entities. The first is the user with a wearable device on him/her that gives input of health-related data on the pulse, walking metrics of speed and distance, sleep duration, etc. The user has full access to his or her data and can share it for treatment purposes. The second the wearable device is the interface to record and store in a timely fashion. The data is synchronized to the cloud on a real-time basis. The third is the healthcare provider giving data for the patient’s treatment, and the fourth is the health insurance layer for verification purpose. The fifth is the blockchain layer that stores the data and gets updated real-time. The sixth is the cloud database that consists of transactional data of user queries and requests.

In [37] continuation to addressing the blockchain issues in cryptocurrencies on secure transactions, the authors mapped the solution to healthcare. They based their system on three aspects: authentication, confidentiality, and accountability. The end target users are researchers, public health authorities, and blockchain miners. Cryptographic techniques are used for user verification, monitoring, data sharing etc. The architecture is designed to integrate with local and existing data storage.
In this [38] model, the researchers designed the system to access the patient information from the wearable device in emergency situations with a private key and a public key. The private key is recognized only through biometric signature of patient. The other features or benefits are decentralized architecture, interoperability, user verification, user monitoring. The further study in this model as indicated by the authors are communication and the authentication protocols.

This model [39] is named Ethereum that gives guaranteed stockpiling of data and ensures user (in this case, the patients) security cryptographically in healthcare on a blockchain architecture. The metrics on which this system is tracked are performance and execution results. The blocks are added with a new patient in the chain and timestamped. There is also user monitoring to prevent malicious activities.

This model [40] focused on a multilevel blockchain-based location sharing scheme in mobile health care technologies to overcome the shortcomings of security and protection and give the real location of the patient. The system consists of a data sender layer, data receiver layer, registration unit and private accessible unit. The sender layer takes in all the patients data checks and encrypts it while the receiver layer authenticates it with the system and stores the data. The registration unit stores the user credentials and handles the log-ins. The private accessible unit ensures the flow of information between two parties on a verified channel.

This model [41] is developed for medical insurance domain in the blockchain framework keeping patients, clinics, insurance companies, and the data storage servers as stakeholders. The model built on Ethereum platform with performance evaluation as an information check guarantee is the critical aspect of medical insurance. The model is built on three layers namely the user, secure system management and secured data storage. The user layer is for authenticated blockchain miners, the system management layer is for secure transactions, and the storage layer is a key layer protected from breach as it could impact the insurance revenues and outgo.

This model [42] focused on solving the problem of identical patient data stored in different locations and multiple databases by blockchain architecture. This model eliminates the replication of records and network congestion. The advantages of the model indicated by the authors are avoiding single point of failure, patients right to access, ease of access to healthcare data and detection of malicious activity on data.

The work [43] Keeping in view the benefits EHR/EMR and diagnosis of patients, the authors have developed a model of healthcare system in a data-sharing scheme. The scheme comprises two blockchains (i) private blockchain (ii) consortium blockchain. Implemented in JUICE the private scheme stores the patient health records while the public scheme generates secure indexes for the data records stored. The data is stored centrally with the authentication of user feature for requested data dissemination.

This model [44] proposes a framework of blockchain in healthcare system for remote patients with wearable devices on them for getting the information. In this model, the miner is selected by the patient for the process to start. The key drawbacks noticed in this model is block validation and authentication protocols details in the architecture.
This [45] model proposes a framework for smart contracts in blockchain for remote patient monitoring. The patient is tracked through sensors for data input after permission. The data validation happens through a consensus mechanism with the system acting only if all the permitted users are present. The key drawbacks noticed in this model is block validation and authentication protocols details in the architecture.

| Author | Model /Project Name | Architecture/Key Features | Applied Area/Industry | Drawbacks /Further Study |
|--------|---------------------|--------------------------|-----------------------|--------------------------|
| Badr et al. [13] | - | Protocol of Pseudonym Based Encryption with Different Authorities (PBE-DA) with blockchain | E-Health Platform For Patients | - |
| Agbo et al. [14] | - | Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) Guidelines and A Systematic Mapping Study Process | Highlights The State-of-The-Art In The Development of Blockchain Applications For Healthcare | - |
| Vazirani et al. [15] | - | Reviewers Identified Studies Via Systematic Searches of Databases Including PubMed, MEDLINE, Scopus, EMBASE, ProQuest, and Cochrane Library with a Total of 71 Studies | Discuss Potential Benefits And Limitations Without Evaluation Of The Model Effectiveness. Some Systems Tested On Live Data | - |
| McGhin et al. [16] | - | Review Of Existing Blockchain Technologies In Smart Contracts, Fraud Detection, And Identity Verification. | Vulnerabilities Like Mining Incentives, Mining Attacks, and Key Management. Unique requirements of healthcare applications. | Potential Research Opportunities |
Gordon et al. [17]: Interoperability Through Five Mechanisms: (1) Digital Access Rules, (2) Data Aggregation, (3) Data Liquidity, (4) Patient Identity, And (5) Data Immutability.

The Transition From Institution-Centric To Patient-Centric Data Sharing.

Zhang et al. [19]: Contributions to “Shared Nationwide Interoperability Roadmap” from the Office of the National Coordinator for Health Information Technology (ONC).

ONC requirements and their implications; FHIRChain - Fast Healthcare Interoperability Resources (FHIR) standard for shared clinical data; FHIRChain-based decentralised app for remote cancer care; Key takeaways.

Kuo et al. [20]: Blockchain Technologies, Benefits, Pitfalls, And The Latest Applications.

Biomedical And Health Care Informatics Researchers.

MIT [26]: MedRec&MedRec 2.0

Data Fragmentation, Interoperability, Patient Focus, and Medical Diagnosis Data.

Patient Contracts and Linking of Patient And Caretaker.

End-point security.

Medical Chain [27]: Medical Chain

Hyper Ledger Fabric for access control and MedTokens.

Marketplace For Negotiation With Third Parties For Data Access.

Non-purchase of tokens and lack of legal qualification for MedToken security.

Patientory [28]: Patientory

HIPAA-compliant data storage systems.

Tokens on this platform are used for storage space or third party contract functions.
| Author(s)                        | Article/Project                                                                 | Method/Technology                                                                 | Key Benefits/Issue                                                                 |
|---------------------------------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Christidis et al. and Bocek et al. [29], [30] | Eliminating The Privacy Issue In Using Blockchains In Internet-Of-Things (IoT) Space | Patient/user privacy and pharma supply chain                                       | -                                                                                |
| Esposito et al. [31]            | Blockchain on existing cloud-based medical data with security                 | EHR/EMR system on the cloud                                                       | Complying to the privacy laws and regulations                                      |
| Omar et al. [35]                | MediBChain                                                                    | Elliptic Curve Cryptography                                                       | Pseudonymity (username and password) and electronic contracts                      |
|                                 |                                                                                | Permission Management Is Implemented With The Decentralisation Of Medical Records By Cryptography | Smart contracts with a Proof-of-Work (POW) algorithm                               |
| Azaria et al. [23]              |                                                                                | Moving Away From Centralisation Of Data, The Data Is Stored In A Distributed Environment Ensuring Better Interoperability Keeping The Heterogeneous Nature Of Healthcare Data | Cryptographic Techniques for user Identity-Check                                   |
| Kaur et al. [32]                |                                                                                | BlockChain Based Data Sharing (BBDS) framework. The System Is Divided Into User, System Management And Storage Layers | Communication and the authentication protocols in this framework                   |
| Xia et al. [33]                 |                                                                                | Healthcare Blockchain Miners                                                       | Research end-users of Healthcare Data                                              |
| Xia et al. [34]                 | MeDShare                                                                       |                                                                                   |                                                                                   |
Existing Database Infrastructure.

The System Is A Membership Service For Healthcare Data Storage, Multiple Nodes, and Application Programming Interfaces (APIs)

Dubovitskaya et al. [24] - Cancer Healthcare Blockchain Miners -

User-Centric Mobile Application And Wearable Devices Synchronized In A Tree-Based and Batching Approaches

Liang et al. [36] - Healthcare Provider and Health Insurance Provider -

Cryptographic Techniques are Used For User Verification, Monitoring, Data Sharing

Nakamoto et al. [37] - Researchers, Public Health Authorities, And Blockchain Miners -

Designed The System To Access The Patient Information From The Wearable Device In Emergency Situations With A Private Key And A Public Key

High et al. [38] - Healthcare Provider Communication And The Authentication Protocols -

Guaranteed Stockpiling Of Data And Ensures User (In This Case The Patients) Security Cryptographically In Healthcare On Blockchain Architecture

Li et al. [39] - Ethereum Healthcare Blockchain Miners -

Multilevel Blockchain-Based Location Sharing

Ji et al. [40] - Healthcare Provider -

Scheme In Mobile Health Care Technologies
| Authors               | Protocol | Medical Insurance Domain | Healthcare Blockchain Miners |
|----------------------|----------|---------------------------|-----------------------------|
| Zhou et al. [41]     | Ethereum | Information Check Guarantee As To The Critical Aspect Of Medical Insurance Built On Three Layers Namely The User, Secure System Management And Secured Data Storage | -                            |
| Fan et al. [42]      | -        | Solving the problem of identical patient data. Eliminates the replication of records and network congestion. | -                            |
| Zhang and Lin [43]   | JUICE    | The Private Scheme Stores The Patient Health Records While The Public Scheme Generates Secure Indexes For The Data Records Stored | -                            |
| Uddin et al. [44]    | -        | A Framework Of Blockchain In Healthcare System For Remote Patients With Wearable Devices | -                            |
| Griggs et al. [45]   | -        | Framework For Smart Contracts In Blockchain For Remote Patient Monitoring | -                            |
|                      |          | All User Consensus-Based Healthcare Blockchain Miners | -                            |
|                      |          | Block Validation And Authentication Protocols Details In The Architecture | -                            |

### 6. Gap Analysis

In overall, it is imperative that there are profound ways in which the system can be more robust and development oriented. However, there are certain conditions in the system that must be more effectively planned in terms of implementation. While it is clear from the blockchain implementation in other verticals, that if planned for effective implementation, the solution can be
resourceful. Still, the gaps like the cost of infrastructure, and the management of the peer-to-peer network holds some significant issues[6].

For instance, in the operational circuit of the blockchain, once a new block hash is created, it is shared among all the peer-to-peer network members for verification. Post the verification and consensus from the peer members, the block is added to the chain successfully. The constraint to be observed is about approval from the number of peer members to approve the transaction. If there are some fictitious nodes in the peer network, then the scope of the fictitious data blocks added to the chain is possible.

Secondarily, the other gap is about transparency in the data view. Though the block might not permit for any change once successfully verified, still the anomaly detection to the system is possible, wherein the peer network independent nodes have tampered.

The case instances that are taken up for the review towards understanding the gaps in the implementation of the blockchain solutions in healthcare domain are more pertinent to the domain, in addition to some of the common problems that are envisaged in the conditions for the usual implementation of the blockchain models. One critical area of the blockchain-related solution implementation conditions is about the IoT devices used to the blockchain system.

IoT based bodily sensors that work as the critical factor that supports the data transmission to the systems if treated as nodes are integral to the blockchain structure. Numerous studies have focused on how the IoT bodily sensors should be more enduring and the ones that are prone to the risk of compromising. If the node level body sensors are prone to malicious attacks, there are potential chances that the data transmitted to the block is a manipulated information, which might impact the conditions of accuracy.

The blockchain system does not rely on any pre-verification process when the record is reaching the block. Only when the record is created to a block, the verification process is initiated. In simple terms, the prevention of tampering to the existing data is possible with the blockchain system, but the scope of manipulated information reaching the block for a record is potentially high.

Such conditions eventually impact the facets on two dimensions. One the time consumed by the distributed nodes that are integral to the system, towards verifying the record hash. The second in terms of seemingly manipulated information entering the block at the genesis record level.

In a scenario of the context mentioned above, when a body sensor implanted into a human body is infected with malware attack, there are potential chances that the data that is transmitted by the system might also have a significant impact if the block hash is created once based on the manipulated data. Considering the enormity and sensitivity related to the data, it is imperative that the security factors of the nodes that are integral to IoT must be taken into account.

The secondary scenario is about the enormity of data that is generated from the implanted devices to the server network. When there are multiple sets of records that are developed for the healthcare system from the implanted devices and the external set of information systems (electronic health records, diagnostic reports, insurance systems etc.) such data must be a comprehensive network sharing. For instance, when the implanted devices to transmit information for the system, it is integral to the blockchain distribution ledger. But the data related to insurance claim verification factually might not require verifying the record, and it doesn’t require the information in its implant.
device memory. Hence there is a need for a more structured model of data formulation wherein the blockchain-based system can be more significant for authentication of information access to the distinct set of information systems integral to the process.

The other dimension is when the electronic health record of a patient has some vital parameter related information of the patient; such inputs are presumably accessible to hospitals, insurance companies and the patient. If the implanted device in the body provides information to the system, then, there is a need for all the nodes in the block to take in to account the structure, and there is an integral need for a more robust structure of authentication.

It is highly important that the factors discussed above are given due attention, and there is an appropriate kind of system integration to overcome some of the key factors discussed as gaps in the system implementation. If such metrics are developed, then the implementation of the system in the healthcare domain can be more robust and can provide significant outcome[9].

7. Conclusion

Information systems security has significant importance as any information breach might be a very challenging issue for many stakeholders associated with the system. Blockchain, overall, can be defined as a system that ensures the transaction data is secured and monitored for amendments or trans positioning of data from one level to the other. Such system shall help the system in having more secured levels of development. It is imperative from the literature that the blockchain is undeniably high levels of ingenious development. Today, across the verticals, the role of blockchain solutions is becoming an impeccable development. In this report, the emphasis was about the blockchain implementation in the healthcare domain. One of the common factors that are discussed in the literature is about the scope for implementing the system effectively, as the data in healthcare is highly sensitive and the vulnerabilities of blockchain system that must be addressed. If the objectives defined in the system could be researched and the necessary outcomes are developed as solutions, implementation of blockchain in healthcare can be more sustainable.

8. References

[1] Underwood, Sarah. "Blockchain beyond bitcoin." Communications of the ACM 59, no. 11 (2016): 15-17.
[2] Crosby, Michael, PradanPattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. "Blockchain technology: Beyond bitcoin." Applied Innovation 2, no. 6-10 (2016): 71.
[3] Wang, Huaiqing, Kun Chen, and Dongming Xu. "A maturity model for blockchain adoption." Financial Innovation 2, no. 1 (2016): 12.
[4] Liu, W., S. S. Zhu, T. Mundie, and U. Krieger. "Advanced block-chain architecture for e-health systems." In 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1-6. IEEE, 2017.
[5] Manguesius, Patrick, Johannes Bachmann, Thomas Healy, SamrendSaboor, and Thomas Schabetsberger. "Blockchains in IHE-Based Networks." Studies in health technology and informatics 251 (2018): 27-30.
[6] XXu, Z., J. Kim, S. Ryu, D. Alevtina, and F. Wang. "secure Electronic Medical Records Sharing Using Block chain: su-i-gpd-j-100." Medical Physics 44, no. 6 (2017): 2822.

[7] Sadiku, Matthew NO, Kelechi G. Eze, and Sarhan M. Musa. "Block chain Technology in Healthcare." International Journal of Advances in Scientific Research and Engineering 4 (2018).

[8] M. Shilpa, E. Rahul Sharma, and M. Sartaj Singh, “Big data analytic on block chain across healthcare sector,” Int. J. Eng. Technol., 2018.

[9] Siyal, Asad, Aisha Junejo, Muhammad Zawish, Kainat Ahmed, Aiman Khalil, and Georgia Sourou. "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives." Cryptography 3, no. 1 (2019): 3.

[10] Gordon, William J., and Christian Catalini. "Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability." Computational and structural biotechnology journal 16 (2018): 224-230.

[11] Cocco, Luisanna, Andrea Pinna, and Michele Marchesi. "Banking on blockchain: Costs savings thanks to the blockchain technology." Future Internet 9, no. 3 (2017): 25.

[12] Yadav, Vinay Surendra, and A. R. Singh. "A Systematic Literature Review of Blockchain Technology in Agriculture." 2017.

[13] Badr, Shaimaa, Ibrahim Gomaa, and Emad Abd-Elrahman. "Multi-tier blockchain framework for IoT-EHRs systems." Procedia Computer Science 141 (2018): 159-166.

[14] Agbo, Cornelius C., Qusay H. Mahmoud, and J. Mikael Eklund. "Blockchain technology in healthcare: a systematic review." In Healthcare, vol. 7, no. 2, p. 56. Multidisciplinary Digital Publishing Institute, 2019.

[15] Vazirani, Anuraag A., OdhranO'Donoghue, David Brindley, and Edward Meinert. "Implementing Blockchains for Efficient Health Care: Systematic Review." Journal of medical Internet research 21, no. 2 (2019): e12439.

[16] McGhin, Thomas, Kim-Kwang Raymond Choo, Charles Zhechao Liu, and Debiao He. "Blockchain in healthcare applications: Research challenges and opportunities." Journal of Network and Computer Applications (2019).

[17] Hölbl, Marko, Marko Kompara, Aida Kamišalić, and Lili NemecZlatolas. "A systematic review of the use of blockchain in healthcare." Symmetry 10, no. 10 (2018): 470.

[18] Abujamra, Ramzi, and David Randall. "Blockchain applications in healthcare and the opportunities and the advancements due to the new information technology framework." Role of Blockchain Technology in IoT Applications 115 (2019): 141.

[19] Zhang, Peng, Jules White, Douglas C. Schmidt, Gunther Lenz, and S. Trent Rosenbloom. "FHIRChain: applying blockchain to securely and scalably share clinical data." Computational and structural biotechnology journal 16 (2018): 267-278.

[20] Kuo, Tsung-Ting, Hyeon-Eui Kim, and Lucila Ohno-Machado. "Blockchain distributed ledger technologies for biomedical and health care applications." Journal of the American Medical Informatics Association 24, no. 6 (2017): 1211-1220.

[21] Salari, Pooneh, and Bagher Larijani. "Ethical Issues Surrounding Personalized Medicine: A Literature Review." Acta Medicafricana 55, no. 3 (2017): 209.

[22] Cruz-Correia, Ricardo, Duarte Ferreira, Gustavo Bacelar, Pedro Marques, and Priscila Maranhão. "Personalised medicine challenges: quality of data." International Journal of Data Science and Analytics 6, no. 3 (2018): 251-259.
[23] Azaria, Asaph, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. "Medrec: Using blockchain for medical data access and permission management." In 2016 2nd International Conference on Open and Big Data (OBD), pp. 25-30. IEEE, 2016.

[24] Dubovitskaya, Alevtina, Zhigang Xu, Samuel Ryu, Michael Schumacher, and Fusheng Wang. "Secure and trustable electronic medical records sharing using blockchain." In AMIA Annual Symposium Proceedings, vol. 2017, p. 650. American Medical Informatics Association, 2017.

[25] Radanović, Igor, and Robert Likić. "Opportunities for use of blockchain technology in medicine." Applied health economics and health policy 16, no. 5 (2018): 583-590.

[26] MedRec 2.0. Available online: https://medrec.media.mit.edu/technical/ (accessed on 4 April 2019).

[27] Medicalchain. Available online: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf (accessed on 4 April 2019).

[28] McFarlane, Chrissa, Michael Beer, Jesse Brown, and Nelson Prendergast. "Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1." Entrust Inc.: Addison, TX, USA (2017).

[29] Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things." Ieee Access 4 (2016): 2292-2303.

[30] Bocek, Thomas, Bruno B. Rodrigues, Tim Strasser, and Burkhard Stiller. "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain." In 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 772-777. IEEE, 2017.

[31] Esposito, Christian, Alfredo De Santis, Genny Tortora, Henry Chang, and Kim-Kwang Raymond Choo. "Blockchain: A panacea for healthcare cloud-based data security and privacy?." IEEE Cloud Computing 5, no. 1 (2018): 31-37.

[32] Kaur, Harleen, M. Afshar Alam, Roshan Jameel, Ashish Kumar Mourya, and Victor Chang. "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment." Journal of medical systems 42, no. 8 (2018): 156.

[33] Xia, Qi, Emmanuel Sifah, AblaSmahi, Sandro Amofa, and Xiaosong Zhang. "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments." Information 8, no. 2 (2017): 44.

[34] Xia, Q. I., Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani. "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain." IEEE Access 5 (2017): 14757-14767.

[35] Al Omar, Abdullah, Mohammad Shahriar Rahman, Anirban Basu, and Shinsaku Kiyomoto. "Medibchain: A blockchain based privacy preserving platform for healthcare data." In International conference on security, privacy and anonymity in computation, communication and storage, pp. 534-543. Springer, Cham, 2017.

[36] Liang, Xueping, Juan Zhao, Sachin Shetty, Jihong Liu, and Danyi Li. "Integrating blockchain for data sharing and collaboration in mobile healthcare applications." In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1-5. IEEE, 2017.

[37] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. http://www.bitcoin.org. Accessed February 11, 2019.
[38] High, Donald R., Bruce Walter Wilkinson, Todd Mattingly, Robert Cantrell, JO'Brien V. John, Brian Gerard McHale, and Joseph Jurich. "Obtaining a medical record stored on a blockchain from a wearable device." U.S. Patent Application 15/840,589, filed June 14, 2018.

[39] Li, Hongyu, Liehuang Zhu, Meng Shen, Feng Gao, Xiaoling Tao, and Sheng Liu. "Blockchain-based data preservation system for medical data." Journal of medical systems 42, no. 8 (2018): 141.

[40] Ji, Yaxian, Junwei Zhang, Jianfeng Ma, Chao Yang, and Xin Yao. "BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems." Journal of medical systems 42, no. 8 (2018): 147.

[41] Zhou, Lijing, Licheng Wang, and Yiru Sun. "Mistore: a blockchain-based medical insurance storage system." Journal of medical systems 42, no. 8 (2018): 149.

[42] Fan, Kai, Shangyang Wang, Yanhui Ren, Hui Li, and Yintang Yang. "Medblock: Efficient and secure medical data sharing via blockchain." Journal of medical systems 42, no.8 (2018): 136.

[43] Zhang, Aiqing, and Xiaodong Lin. "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain." Journal of medical systems 42, no.8 (2018): 140.

[44] Uddin, Md Ashraf, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. "A Patient Agent to Manage Blockchains for Remote Patient Monitoring." Studies in health technology and informatics 254 (2018): 105-115.

[45] Griggs, Kristen N., OlyaOssipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson, and ThaierHayajneh. "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring." Journal of medical systems 42, no. 7 (2018): 130.

[46] H L Gururaj, A Manoj Athreya, Ashwin A Kumar, Abhishek M Holla, S M Nagarajath, V Ravi Kumar “A New Era of Technology”, Cryptocurrencies and Blockchain Technology Applications, May 2020, Wiley Digital Library https://doi.org/10.1002/9781119621201.ch1

[47] H L Gururaj, A Manoj Athreya, Ashwin A Kumar, S M Nagarajath, V Ravi Kumar “Adoption of pets in distributed network using blockchain technology”, August 2020, International Journal of Blockchains and Cryptocurrencies, Inderscience Publishers, https://doi.org/10.1504/IJBC.2020.108996