iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** I **Month of publication:** January 2023

DOI: https://doi.org/10.22214/ijraset.2023.48576

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue I Jan 2023- Available at www.ijraset.com

An Approach for Implementing of Electronic Health Records Management using Blockchain Technology

N. Nuthan Rajeshwar Rao[1], P. Sai Shashank Reddy[2], G. Jashwant[3], M. Sucheth[4], Md. Khaja Baba[5]
[1, 2, 3, 4, 5]*Computer Science and Engineering Department, Mahatma Gandhi Institute of Technology*

Abstract: ***Data accessibility refers to making sure that users have unrestricted access to information, whereas data privacy refers to making sure that users have control over access to information. Data accessibility and privacy conflicts are common, and the healthcare industry is one where they are particularly crucial. In this post, we talk about how blockchain technology and smart contracts could be useful in various common situations involving data access, data management, and data Interoperability for the particular healthcare area. We then suggest developing a sizable information architecture based on smart contracts as information intermediaries to access electronic health records (EHRs). Our key contribution is how we frame the problems of data accessibility and privacy in healthcare and how we suggest a blockchain-based integrated architecture.***
Keywords: Blockchain, health records, electronic health records, accessibility, and smart contracts

I. INTRODUCTION

Interoperability in the field of data health is still a challenge. The fundamental issue is how to enable open access to practical data (health data), while protecting individual privacy, maintaining anonymity, and preventing data misuse.

Smart contracts and blockchain technology [Nakamoto 2008] appear to offer an intriguing and creative solution to maintain references to Electronic Health Records (EHRs). By using this technology, patients could have more control over their own data while providing health professionals and institutions, such as hospitals, access to patient data managed by other organisations. Ensuring privacy and interoperability, blockchain has the potential to enhance EHR systems.

This article investigates the use of blockchain and smart contracts to enhance EHR. To start, we go over some non-technical factors that help health data make sense. Then, we suggest a design that can enhance existing EHR systems. Our objective is to make patient data accessible securely so that a third party cannot access it. Only the patient, healthcare professionals, and/or institutions should be involved without permission.

We introduce one example that is particularly pertinent to more clearly explain and explore these issues:

- Simple example. While having a medical appointment at institution Z, patient X needs some medical data, but the data was created during a prior appointment between X and Y and is maintained by professional/institution Y. In this case, X is typically a common person. Y and Z are two different medical specialists or hospitals.

The scenario described above is somewhat common, yet it raises a variety of technical and non-technical concerns. How can X's health data be located and made accessible is the initial query. This suggests that a discovery service exists and that Y and Z can communicate with one another. What privacy limitations must be followed is the second query. For instance: 1) data privacy, 2) control over who has access to each piece of data, 3) faith in medical institutions, etc. Additionally, even if all data are human accessible, such as in PDF format, standardising data formats is an issue. Data accessibility refers to making sure that information access is unrestricted, whereas data privacy refers to making sure that users retain control over access to personal information [Pavlou 2011].

Conflicts between accessibility and privacy are inevitable, and the healthcare industry is one where they are particularly pertinent. Most of the time, patients require the treatment of many doctors and institutions, all of which should have access to each other's clinical notes and patient information [Reti et al. 2010]. Institutional or personal health records are not necessarily interoperable, and institutional health records are not always accessible to other institutions [Detmer et al. 2008]. These problems are well-known in the healthcare industry and are related to care coordination, a major issue in medicine (see, for instance, Klein et al. 2015). In another scenario, if the patient's medical condition prevents her from being able to grant permission to her records (for example, because the patient is unconscious), we can think about a "break the glass" mechanism,

Where a health professional is given permission to access her records, given an explicit account of the patient's condition and presentation of the professional's necessary credentials, as well as publicly available information stating that the professional is authorised to do so.

To reduce information curation costs and the need for trust in fewer third-party organisations, it is in the patient's best interest that these situations use the fewest possible mediating institutions.

A blockchain-based solution can enable widespread accessibility, maintain data privacy, lower curating and mediation costs, and offer trustless confidence in information networks. In the sections that follow, we go over blockchain-related activities, data accessibility, and privacy concerns in the context of implementing and maintaining a global EHR built on a decentralised blockchain architecture. We also present a sketch of the system's architecture, which may include all of these features, as well as any additional guiding ethical and openness principles.

II. DISTRIBUTED AND SECURE COLLABORATION WITH BLOCKCHAIN

Blockchain technology was most widely used in cryptocurrencies like Bitcoin [Nakamoto 2008]. They've been suggested as a way to develop additional decentralised applications more recently [Ferrer 2016, Lazarovich 2015, Peterson et al. 2016], Lewenberg et al. (2015), and Norberhuis (2015). A distributed ledger, which functions as a database and contains data on the history of transactions involving various agents, is the foundation of blockchain technology. Groups of agents (chosen in accordance with various policies, depending on the application domain) continuously audit it. Each auditing's outcome is recorded in a block and transmitted to the network. Blocks are sequentially added to the ledger and join together in a chain using cryptography. It is simple to identify attempts to tamper with the blocks or change their arrangement. According to a predetermined set of rules, the entire community has the option to approve or reject any block's dependability. An agent always selects the longest chain of valid blocks (or the oldest one, if they are equal in length) when receiving multiple valid updates to their local copy of the ledger, discarding any conflicting and less significant chains. Even in situations where propagation is sluggish due to significant network latency, consensus will finally be obtained thanks to this theoretically straightforward approach. Similar to this, malevolent nodes may attempt to add entries to the ledger with good intentions, but the community will simply ignore their blocks and chain, thereby forcing them to follow the rules. If the community approves auditing, the ledger—which can include recent, previously unconfirmed transactions—is replicated across the agents. If not, the largest accepted piece of the ledger is copied with details regarding discrepancies and necessary actions, whose results are then recorded as new transactions to be audited during subsequent rounds of verification. As a result, it is possible to imagine a blockchain-based solution that would ensure information accessibility in any kind of large-scale system. Given that (1) peers are required to store copies of the ledger of interactions and (2) transactions and blockchains per se must be distributed across the network of peers, the distribution of health records across a network of healthcare agents can be accomplished most effectively using this technology, provided that solutions are provided for the latency and storage requirements associated with it.

A blockchain-based platform for entirely decentralised applications is called Ethereum [Wood 2014].The foundation of it is the concept of smart contracts, which are protocols that define action steps so that peers can interact with one another. It is possible to implement pertinent agents for information management using smart contracts. Rules for restricting user access to the contents of encrypted health information could be included in smart contracts, for instance. This might make it possible to use smart contracts to build a privacy layer into a distributed information system. The architecture suggested in this article is based on the present Ethereum platform and the concept of using smart contracts to automate the workflow of health data.

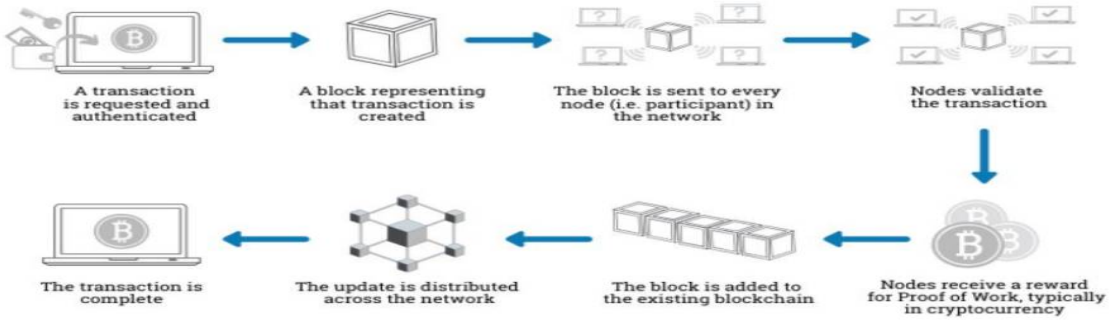


Figure 2.1 Overview of completing a transaction

The qualitative analysis process looked at 67 papers' abstracts. Finding common themes required a deeper examination of the complete articles that were chosen for inclusion. Patient-centered care, value-based systems, and managing health IT are all factors in healthcare. Sustainability, electronic health records, and the security of health data are all factors in the blockchain. Articles about blockchain programming and the bitcoin market were prohibited. There were still 38 articles available for examination.

III. REQUIREMENTS FOR AN OPEN AND GLOBAL EHR SYSTEM

In this section, we go over a few difficult needs for EHR systems and how blockchain technology and smart contracts could be able to help.

A. Data Accessibility And Management

Accessibility to health records is a significant issue in the scenarios examined in this paper. Traditional approaches would be predicated on the formal and social acceptability of one (or a network of) mediating institutions, who would be in charge of keeping and curating health records and regulating access to them in accordance with existing laws and contracts.

The following are two pertinent concerns with regard to the hiring of such mediators:

1) Financial concerns, as the upkeep of a dependable infrastructure to store health records on a broad scale and regulate access to them properly requires significant resources, even when the mediators are nonprofit organisations.
2) Trust-related difficulties; in order to be acknowledged as information keepers, these mediators must be considered as dependable and trustworthy by all parties.

The alternative of using a decentralised network of mediators to store and handle information has been made possible by blockchain technologies. With this technology, it is not necessary to believe in any particular mediator because the greater and less organised the network of mediators is, the more dependable the collective behaviour of these mediators can be taken into account. The idea of "trustless trust" is thus introduced by blockchain technologies, where users of an information system can place their trust in the system as a whole without having to recognise or have faith in any particular peer.

B. Privacy levels and anonymization

Information about a person's personal health should be kept private. To guarantee that only the patient's own healthcare providers and others who have the patient's express consent to see their records have access, an EHR system must incorporate privacy policies.

However, certified institutions in charge of managing public healthcare should have access to aggregate and de-identified data so they may monitor and stop the spread of diseases, for example. To address various privacy concerns, a commitment and encryption layer must be included in the solution.

An exception is when a patient is unresponsive, in which case access to personal data should also be taken into account (e.g. because she is unconscious). These exceptions call for the involvement of mediating third-party institutions or other care providers, who must record, preserve, and administer the exceptions (declared by people), as well as credentials, and the circumstances that call for extraordinary access to private information.

Additionally, authorities in charge of public healthcare must have access to anonymised aggregate data. Data anonymization in this context is a type of information sanitization with the goal of protecting privacy. To ensure that the individuals to whom the data pertains remain anonymous, personally identifying information is either encrypted or removed from data sets. However, anonymization does occasionally provide a danger of unfavourable societal repercussions [Taylor 2016]. Prior to signing up for any information management system, patients must be made fully aware of the corresponding hazards.

As a result, privacy needs to be divided into smaller layers, with access to each layer being governed by a different set of guidelines. For instance, carefully crafted templates can be used to make sure that data is saved in the proper sub-layers while constructing an electronic health record.

Individually identifiable data may be on a different layer from anonymized aggregate data, and may only be disclosed with the direct consent of the patient.

By automating the structuring of data in various levels of privacy and detail, smart contracts may be an aid in the process of data cleansing. Consensus algorithms on the blockchain may also make it possible to develop "break the glass" solutions without the need of a third party intermediary.

IV. A GENERAL ARCHITECTURE FOR A GLOBAL SCALE EHR BASED IN BLOCKCHAIN

In light of the aforementioned difficulties with data accessibility, privacy, morality, and the value of openness, we present an EHR architecture built on blockchain and smart contracts that might make health records interoperability feasible and secure on a worldwide scale.

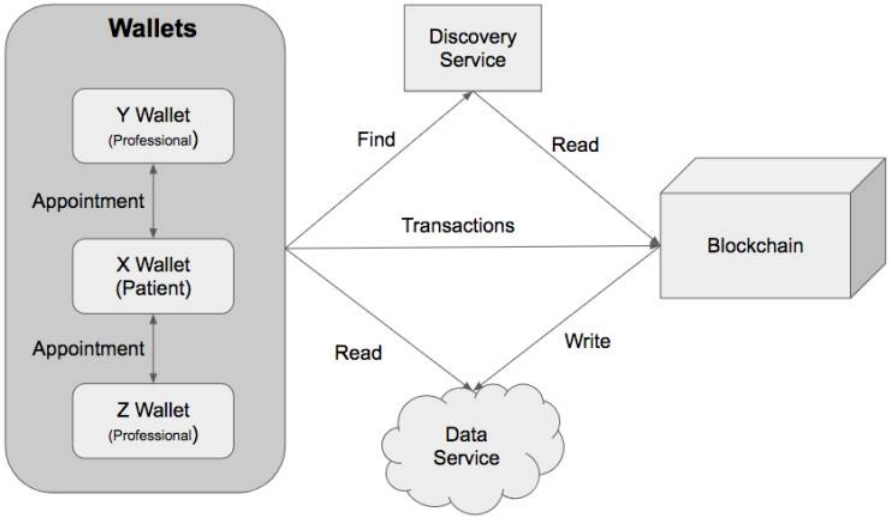


Figure 4.1 The elements of basic architecture

1) *Blockchain:* A distributed ledger with smart contract execution capabilities. This component is in charge of keeping track of references to medical transactions, including doctor's appointments, diagnostic tests, prescription medications, etc. In conclusion, a block in a cryptocurrency system consists of financial transactions. Each transaction's format is described in Section IV. *A*. A block may have links to health data in an electronic health records privacy layer. For instance, when a patient X is seen by a doctor in the hospital Y, a transaction is recorded in the ledger indicating that Y has access to the patient's data.
2) *Service For Data:* A service that stores data and is required to retain the medical records. Each file in this proposal's cloud file system belongs to party X and can be read by party Y 3. For instance, you may use Dropbox, Google Drive, and Megadrive, which are all well-known cloud storage options. To be used in our architecture, the data service must provide cloud access, file access control, and APIs to add and remove reading access to the files.
3) *Wallets:* The private and public cryptographic keys of a user must be stored in an electronic wallet. Users are identified in the solution using the public key. The password and email used to access the data service are likewise stored in the wallet. The system can be accessed using the wallet as its default user interface.
4) *The Discovery Service:* is a supplemental, optional technology that speeds up information search. It serves as an index to the data kept on the blockchain. For instance, the discovery service provides a list of blockchain transactions that belong to a patient named X, identifiable by his public key X+. Additionally, it must provide a way to locate X and Y given a pointer to a data file. A NoSQL database that maintains a view of the blockchain with eventual consistency could be used to offer this service.This component has no security flaws because it only reads the blockchain, and the answers to its queries can be easily confirmed by local copies of the blockchain. Additionally, the Discovery Service might develop to provide fundamental services for a professional search.

The architecture separates data storage from transaction control, which is accomplished using a blockchain ledger (Data Service). All data might theoretically be stored in the ledger in a solution, however this is not practical because to performance issues.

This architecture's practise of giving consumers control over data management is one of its features. The patient is the owner of the data and has the right to delete or limit access to it at any time.

The collection of smart contracts forms the basis of the architecture. They are accountable for:

- Storing a new transaction in the ledger and are kept in the books.
- Obtaining and processing requests for access;
- Recording all authorised access to data.

A. Transactions

The fundamental piece of data that the system manipulates is a health transaction. There are specified the following categories of transactions:

1) *New Record:* With this transaction, a fresh record is added to the ledger. It has the following fields: timestamp, X+, Y+, content metadata, content public data, link, and hash (data).

Where: The public data and metadata are optional fields; the link is the location of the electronic health data that is stored in the cloud, encoded so that only X or Y could decode it (for instance, the sensible parts of the file can be encoded using key K, but the file also contains X+(K) and Y+(K)). The field hash(data) enables the accuracy of the data content to be verified; it is crucial to ensure that the information has not been altered.

2) *Request Access:* is a tool established by Z to ask for access to stuff that belongs to X.

It includes a timestamp: a Z +, an X +, and a Z (X+(link)). To establish Z's identification, use the phrase Z (X+(link)). Because the link is encoded with X+, it should be noted that only X can allow access to the data.

In response to an Access Request, X generated the object Access Granted. Timestamp, X+, Z+, and link are all present. It should be noted that the link will include a copy of the original value with permissions set to Z.

B. Data Ownership

The patient X is the data owner in this system. Each user is assumed to set up a cloud file system in the wallet. The user can delete his or her personal health information, revoke access to it, but he or she cannot delete a transaction from the ledger

C. Wallets

The solution is based on a technique called personal health wallets, which securely store a patient's identification on a blockchain. The Wallet is devoid of Only a public key is revealed in the blockchain; a patient is not identifiable there. However, it is well recognised that looking into additional factors can reveal an identity. 2017 [Goldfeder et al.]

D. Smart Contracts

A smart contract is a piece of computer code that is recorded on the blockchain and can be run on a virtual machine. They can be used, for instance, to start a new transaction, resolve transactional conflicts, send alerts, etc. Contracts should verify the transaction requests in our design. The software component that sends a transaction to be stored on the blockchain after it has been validated is the contract, in actuality. We predict the necessity of, at least, the following contracts:

1) Create New Record
2) Process Access Request

It is possible to create additional contracts to execute complex anonymization procedures, pay patients for data access granted, etc.

V. CONCLUSIONS

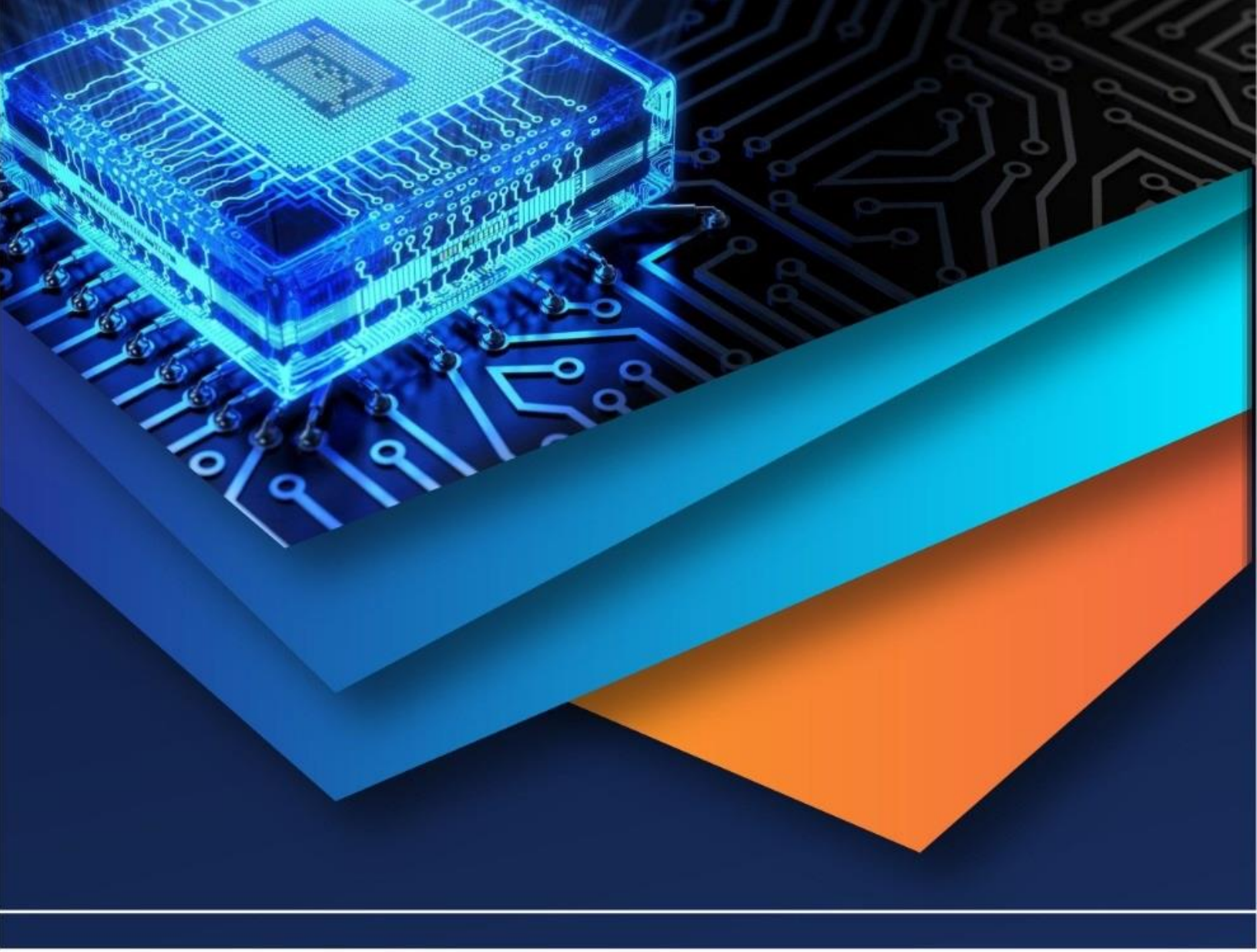
Despite recent IT advancements, few healthcare organisations today offer data linkage between departments. The primary healthcare scenarios of care coordination and health information management are utilised in this work, and a secure data exchange architecture is also proposed. In our idea, the patients own all data. In order to achieve security, high availability, fault tolerance, and better trust, it also depends on blockchain technology and widely utilised cloud storage services. The suggested architecture is adaptable to take both technical and moral aspects into account. It advances the discussion of each of these concerns and, in doing so, moves us closer to finding answers to the conflicts between data accessibility and privacy. However, it does not resolve these conflicts or suggest remedies. In the future, after a trustworthy health data network has been established, the activity of granting data access could be transferred to the blockchain, opening up new possibilities for the management of health data.

VI. FUTURE WORK

In the near future, we want to put the proposed architecture, depicted in Section 5, into practise as a functional prototype. A straightforward mobile wallet created in Android should be a part of this minimal implementation, together with contracts created using the Ethereum foundation (Wood 2014). In addition to validating the architecture, one of our objectives is to objectively assess how many transactions the blockchain can sustain. The ability of the Ethereum development framework to describe complicated computer models, which are required for the implementation of actual smart contracts in the healthcare industry, is another factor that needs to be considered.

REFERENCES

[1] A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.
[2] G. Jetley and H. Zhang, ''Electronic health records in IS research: Quality issues, essential thresholds and remedial actions,'' Decis. Support Syst.,vol. 126, pp. 113–137, Nov. 2019.
[3] K. Wisner, A. Lyndon, and C. A. Chesla, ''The electronic health record's impact on nurses' cognitive work: An integrative review,'' Int. J. Nursing Stud., vol. 94, pp. 74–84, Jun. 2019.
[4] M. Hochman, ''Electronic health records: A ''Quadruple win,'' a ''quadruple failure,'' or simply time for a reboot?'' J. Gen. Int. Med., vol. 33, no. 4, pp. 397–399, Apr. 2018.
[5] Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. In Open and Big Data (OBD), International Conference on, pages 25–30. IEEE.
[6] Barrue, C., Cort ´ es, A., Moreno, J., and Cort ´ es, U. (2015). Using multi-agent systems to mediate in an assistive social network for elder population. In Artificial Intelligence Research and Development: Proceedings of the 18th International Conference of the Catalan Association for Artificial Intelligence, volume 277, page 120. IOS Press.
[7] Culnan, M. J. (1984). The dimensions of accessibility to online information: Implications for implementing office information systems. ACM Transactions on Information Systems (TOIS), 2(2):141–150.
[8] Dehling, T., Gao, F., Schneider, S., and Sunyaev, A. (2015). Exploring the far side of mobile health: information security and privacy of mobile health apps on ios and android. JMIR mHealth and uHealth, 3(1).
[9] Detmer, D., Bloomrosen, M., Raymond, B., and Tang, P. (2008). Integrated Personal Health Records: Transformative Tools for Consumer-Centric Care. BMC Medical Informatics and Decision Making, 8(1).
[10] Ekblaw, A., Azaria, A., Halamka, J. D., and Lippman, A. (2016). A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data. In IEEE Open & Big Data Conference, volume 13, page 13.
[11] Fadhil, M., Owen, G., and Adda, M. (2016). Bitcoin network measurements for simulation validation and parameterisation. In Proceedings of the Eleventh International Network Conference (INC 2016), page 109.
[12] Fadhil, M., Owen, G., and Adda, M. (2016). Bitcoin network measurements for simulation validation and parameterisation. In Proceedings of the Eleventh International Network Conference (INC 2016), page 109.
[13] Klein, D. M., Fix, G. M., Hogan, T. P., Simon, S. R., Nazi, K. M., and Turvey, C. L. (2015). Use of the Blue Button Online Tool for Sharing Health Information: Qualitative Interviews With Patients and Providers. Journal of Medical Internet Research, 17(8):e199.
[14] Liu, P. T. S. (2016). Medical record system using blockchain, big data and tokenization. In Information and Communications Security, pages 254–261. Springer.
[15] Mann, S. P., Savulescu, J., and Sahakian, B. J. (2016). Facilitating the ethical use of health data for the benefit of society: electronic health records, consent and the duty of easy rescue. Phil. Trans. R. Soc. A, 374(2083):20160130.
[16] Shrier, A. A., Chang, A., Diakun-thibault, N., Forni, L., Landa, F., Mayo, J., and van Riezen, R. (2016). Office of the national coordinator for health information technology US department of health and human services.
[17] Ryoo, J., Rizvi, S., Aiken, W., and Kissell, J. (2014). Cloud security auditing: challenges and emerging approaches. IEEE Security & Privacy, 12(6):68–74.
[18] Taylor, L. (2016). No place to hide? the ethics and analytics of tracking mobility using mobile phone data. Environment and Planning D: Society and Space, 34(2):319–336.
[19] Norberhuis, S. D. (2015). MultiChain: A cyber currency for cooperation. PhD thesis, TU Delft, Delft University of Technology.
[20] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY