Blockchain Based Platform for Healthcare Information Exchange

R. H. Bhangale[1], D. G. Agrawal[2]

[1] *PG Student [CE], Dept. of ECE SSGB College of Engineering & Technology, Bhusawal, Maharashtra, India*

[2] *Assistant professor, Dept. of ECE SSGB College of Engineering & Technology, Bhusawal, Maharashtra, India*

ABSTRACT

Current trend in healthcare industry is to shift its data on the cloud, to increase availability of Electronic Health Records (EHR) e.g. Patient's medical history in real time, which will allow sharing of EHR with ease. However, this conventional cloud-based data sharing environment has data security and privacy issues. This proposes a distributed solution based on blockchain technology for trusted Health Information Exchange (HIE). In addition to exchange of EHR between patient and doctor, the proposed system is also used in other aspects of healthcare such as improving the insurance claim and making data available for research organizations. Medical data is very sensitive, in both social as well as legal aspects, so permissioned block-chain such as Hyperledger Fabric is used to retain the necessary privacy required in the proposed system. As, this is highly permissioned network where the owner of the network i.e. patient holds all the access rights, so in case of emergency situations the proposed system has a Backup Access System which will allow healthcare professionals to access partial HER. The Process of the Blockchains used architecture depends on the entities participating in the constructed chain network. Although the use of Blockchains may reduce redundancy and provide caregivers with consistent records about their patients, it still comes with few challenges which could infringe patients' privacy, or potentially compromise the whole network of stakeholders. Blockchain offers the opportunity to enable access to longitudinal, complete, and tamper-aware medical records that are stored in fragmented systems in a secure and pseudo-anonymous fashion.

Keyword : - *Smart Contracts, Healthcare including Block Chains, Interoperability of Healthcare.….*

---

1. INTRODUCTION

In Healthcare Information Exchange System, various Healthcare entities like Doctor, Pharmacist, Medical Lab in charge and insurance company may have to submit transactions which may result in change in contents of the Electronic Medical Records (EMR). These EMR's are critical and highly sensitive should be known and trusted by other participants.

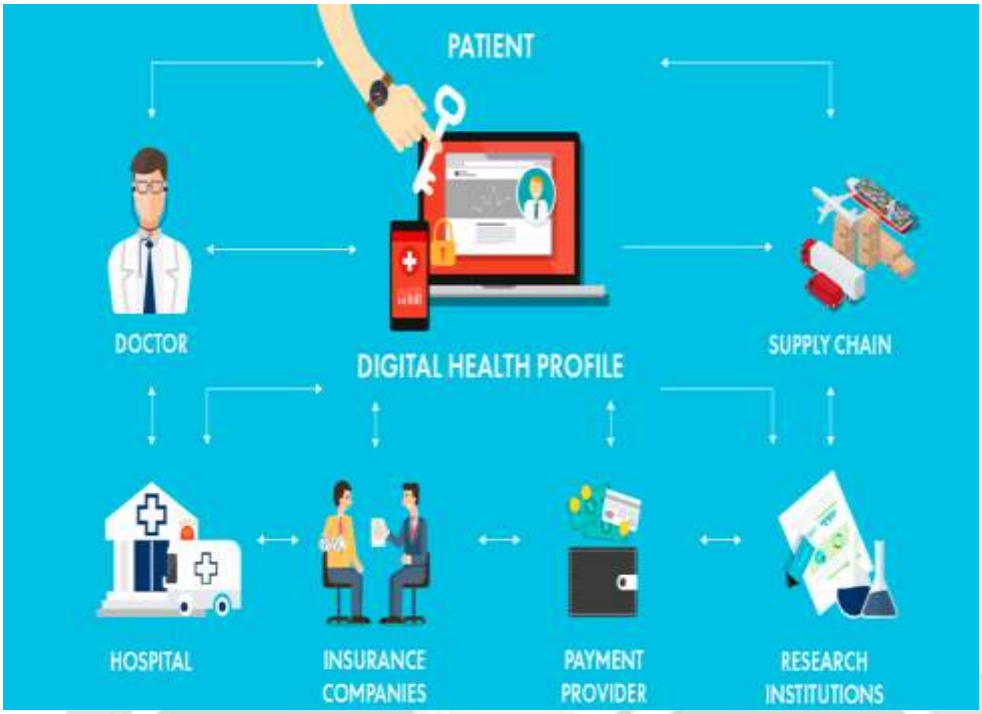

Fig. 1 -Blockchain In Healthcare and Life Science Eco System

In fig. 1 shows the blockchain in healthcare and life science eco system in this patient's medical information which needs to secured. It requires that the participants performing transactions Centralization does not guarantee integrity and data various entities present in the healthcare using blockchain. security so; this proposes a distributed solution to implements a HIE System to share EMR's between Blockchain is a distributed ledger which is used for making logs and storing every transaction block in distributed ledger i.e.whenever a participant cryptographic methods which will allow every node in the network to participate in the interaction (e.g. store information, exchange of information, and view that information), without having prior trust between the participants of the network. There is no central authority in a blockchain system instead, transaction blocks are recorded and distributed to all the peers in the network. So, all participants in the network will know every interaction with blockchain and requires it to be verified before adding to the blockchain, which will enable trust-less interaction between the peers in the network. The block once added to the blockchain can neither be deleted nor updated i.e. it is immutable. In a blockchain based HIE, the patient has the ownership of the medical records, in contradiction to traditional architecture, where a central authority controls accesses and distributes data across network. In this system medical record access is permitted to only limited healthcare entities (people or organizations). Data shared across the blockchain network enables near real e updates across all healthcare entities. Distributed ledger allows secure access to patient data. Data redundancy is reduced as the same copy of data is available to all peers in network. Privacy and confidentiality in blockchain network is maintained by restricting few nodes to access data. In fig. 1 shows the blockchain in healthcare and life science eco system in this

1.1 Hyperledger fabric to support private data

The proposed system requires that some information to be private to some participants and should not be seen by other participants in the network, for e.g. the research organizations and insurance companies need not to know all the transactions in the network. The other permissioned blockchain network requires that all participants should have same view of the distributed-ledger, which makes it difficult to support private data for various different

participants whereas Hyper-ledger fabric provides a way to keep certain data/transactions confidential among a subset of members in network.

2. LITERATURE REVIEW

Blockchain was originally introduced as a mechanism to power Bitcoin, but has now evolved to the point of being referred to as a foundational technology for multiple decentralized applications [5]. Blockchain is being touted as a useful technology for managing sensitive data, especially within the sectors of healthcare, medical research and insurance. the healthcare system to be inclusive of contact-based and technology-based remote monitoring services extended by constituent service providers in an effort to promote, maintain or restore the health of beneficiaries [7]. In the field of healthcare, privacy and security breaches are purportedly increasing every year, with over 300 breaches reported in 2017 and 37 million medical records affected between 2010 and2017. The increasing digitization of healthcare has further led to the acknowledgment of concerns related to secure storage, ownership, sharing of patients' personal health records, and allied medical data [3]. Blockchain has been suggested as a way to solve critical challenges faced by healthcare, such as secured sharing of medical records and compliance with data privacy laws [3].

2.1 Blockchain technology

Blockchain is a distributed public ledger database that is maintained by a network of verified participants or nodes and stores immutable blocks of data that can be shared securely without third-party intervention [2]. Data are preserved and recorded with cryptographic signatures and use of consensus algorithms that are enacted as key enablers of its application (Mendling et al., 2018). This ability for data preservation is a significant reason that has driven the use of blockchain in healthcare, wherein a significant amount of data is subject to extensive exchange and distribution. The evolution of blockchain technology and its application in diverse contexts has occurred in various phases. The first phase of blockchain evolution was related to cryptocurrency and the second pertained to the application of smart contracts in areas such as real estate and finance [9]. The third generation of evolution was focused on the applications of blockchain in nonfinancial domains such as government, healthcare, and culture. Additionally, driven by innovative technological features such as data immutability, blockchain is now considered to be in its fourth stage of evolution with the incorporation of artificial intelligence. Blockchain's asserted diversity in its scope of applications may be attributed to its potential for creating decentralized (Silva et al., 2019) and trustless transaction environments (Zhang et al., 2018). The healthcare industry is a prime candidate for blockchain technology; as blockchain has the potential to address critical concerns, such as automated claim validation and public health management. This technology may allow patients to own data and choose with whom it is shared, thereby addressing extant concerns about data ownership and sharing [2].

Concurrently, it enables data records to be unified, updated, securely exchanged, and accessed in a timely by appropriate authorities with the use of consensus protocols. This is a major advantage afforded by the application of blockchain technology within the healthcare space because current practices require data to be stored with third parties. Finally, blockchain can potentially bring transparency to data management processes (Ito et al., 2018) while also reducing the chances of data mishandling or misuse because of possible human error [1]. Despite the positive connotations of blockchain's effect on societal and business transformation, there seems to be a debate on its prevalent advantages and derived benefits in comparison to previously established expectations. A recent report suggests that although organizations will undertake significant investments in implementing blockchain-based technologies in the future, they will likely adopt a cautiously pragmatic approach because of a prevalent beliefthatthe benefits may be over-hyped. It may be said that this technology is yet to meet its touted expectations, a fact that may be attributed to certain challenges to the widespread implementation of this technology, especially in terms of regulatory barrie [6]. Another important challenge in promulgating the deployment of blockchain is the unfamiliarity of the public and individual users, such as patients or doctors, with the way this technology works, its technical features or its benefits for data management. Iansiti and Lakhani (2017) suggest that due to social, organizational, and implementation barriers, such as security or governance, significant time may be required for blockchain to generate the expected levels of business transformation. This may be additionally compounded by a general uncertainty about blockchain's usage with respect to legal compliance and government regulations. Current research is focused on aiding the operational evolution of blockchain and accelerating its prevalence by addressing these challenges and barriers [4].

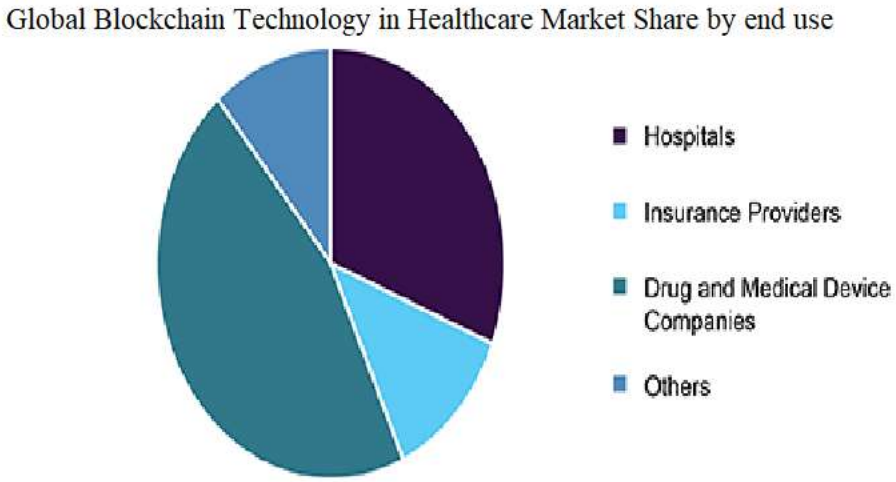

Fig. 2- Blockchain Technology in Healthcare Market Share by End Use

Drug and medical device company segment accounted for the major market share in 2018, owing to the rising adoption of technology for essential functions such as verifying the authenticity of the returned drug, counterfeit prevention, compliance with pharmaceutical supply chain, transparency, and traceability in clinical trials, and improving reliability and quality of clinical trial data.

The hospitals segment is expected to grow at a considerable rate owing to the growing adoption of the technology in hospitals such as the Massachusetts General Hospital (MGH). Healthcare institutions and hospitals are now working on storing patient's data to safeguard the smooth working of the system. This not only helps in classifying new and old patients but also leverages existing records to complement the doctor's appointment. Furthermore, the technology will also prevent vital information, such as payment details, address, phone number, against data breaches, and cyberattacks. The technology is expected to work in favor of the biggest threat in the current world - data security. For instance; the ransomware attack, on the Fetal Diagnostic Institute (FDI) breached over 40,000 patient's data in June 2018. Furthermore, UnityPoint Health, in July 2018, announced that data of over 1.4 million patients was breached by a phishing attack. Such incidences of data breaches can be reduced or eliminated through the integration of blockchain technology in the healthcare industry.

3. SYSTEM DESIGN

3.1 ARCHITECTURAL DESIGN

An architectural design consists of different components as shown in Figure 3 This section presents the structure and functionality of a case study DApp for Smart Health (DASH)2 we developed to explore the efficacy of applying Blockchain technology to the healthcare domain. This prototype was implemented on an Ethereum test Blockchain to emu- late a minimal version of a personal EHR system. It provides a web-based portal for patients to self-report and access their medical records, as well as submit prescription requests. DASH also includes a staff portal for providers to review patient data and fulfill prescription requests based on permissions given by patients. Figure shows the structure and workflow of DASH.

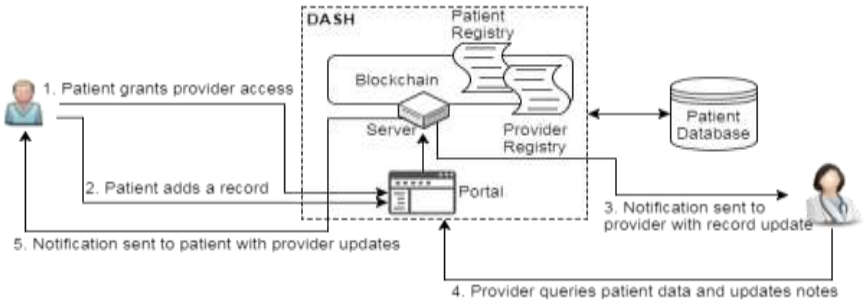

Fig. 3- Architecture Design

To develop a totally localized system needs belief on many parts, like third party establishments, agents and therefore the data network alone. Here, we tend to state that elementary to achieve the required level of trust within the system often outlined as a stress on clearness and free, unrestricted access to data and data, still as cooperative or cooperative management and decision making instead of a central authority. Openness for mentioned to be the other of secrecy. a minimum of four totally different aspects of openness helpful in an exceedingly world EHR and also are gift in blockchain technology: the open or free package, open ethical standards, open kind of data, and open mode of innovation. We tend to show every of those aspects within the next paras.

- Despite the system design incorporated in an exceedingly world EHR, this technique will get pleasure from the inclusion of open supply package to confirm that data is processed in trustworthy ways in which.
- Similar arguments regarding auditability and certification additionally apply to the adoption of open standards to cypher, exchange and transfer data. Additionally, to use open standards is inherently vital to the system integration.
- Open information isn't needed within the specific system pro-posed, as we've got sensitive information moving across a loop of peers. However, the open information is fascinating as a supply of data to grasp network dynamics. For instance, it should be wont to add a social facet within the system, i.e., sanctioning agents to permit or refuse data the utilization of data to an establishment counting on its name or its public perceived belief. In different words, though open information isn't a main feature within the system, and this will be however a strong tool for up its coming releases. A general Architecture for Open architecture for EHR based on blockchain: Fig:

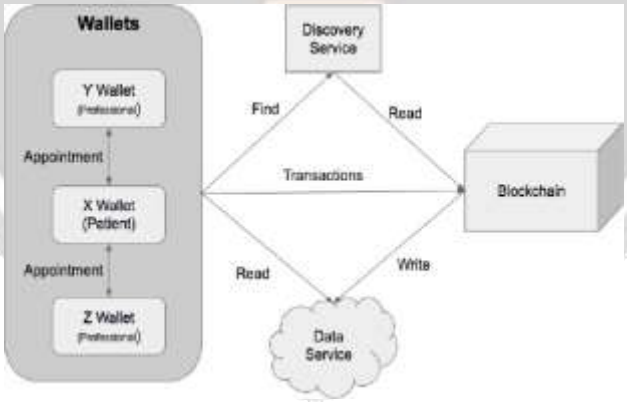

Fig. 4-Open architecture for HER

Description on components:

Blockchain: A distributed ledger can execute smart contract. They record references for health transactions like examination, appointment and medications. It is described in cryptocurrency system. In block of a privacy layer, it contains a pointer to health information of patient. If a patient X is observed by doctor in a hospital Y, then a transaction is appended to Y as if transaction is accessible to information of X.

Data Service: It can store necessary information about health records. They can be implemented using cloud services like Drobox, Google Drive etc.…

Wallets: It has the capability to store user's private and public keys. Email and other credentials are stored with the wallet. It serves as an interface to access the entire system.

Discovery Service: Non-mandatory and other credentials are stored in discovery service. Information stored in Blockchain is indexed using this. This is capable of listing all the services offered to patient X in the listing format.

NOSQL can be used for implementing this. Services offered by ledger includes the following: Storing a transaction, Accessing and processing requests and Registration of all transactions for which access is granted.

Transactions: It is the basic unit of information stored in the system as per the above architecture. The following are the transaction types:

A New transaction creates an entry in the ledger. It contains transitive closures, timestamp information of transaction, link, public profile etc…

Request Access is the record entry listing the request to access the content of patient record X and also lists for those who were granted access.

Notification, these are special information stored along with a transaction.

Smart contracts: It is a program stored in the blockchain and run on virtual system. They actually manage transactions.

3.2 Class diagram

Class diagrams are used in both the analysis and the design phases. During the analysis phase, a very high-level conceptual design is created. At this time, a class diagram might be created with only the class names shown or possibly some pseudo code-like phrases may be added to describe the responsibilities of the class. The class diagram created during the analysis phase is used to describe the classes and relationships in the problem domain, but it does not suggest how the system is implemented. By the end of the design phase, class diagrams that describe how the system to be implemented should be developed.

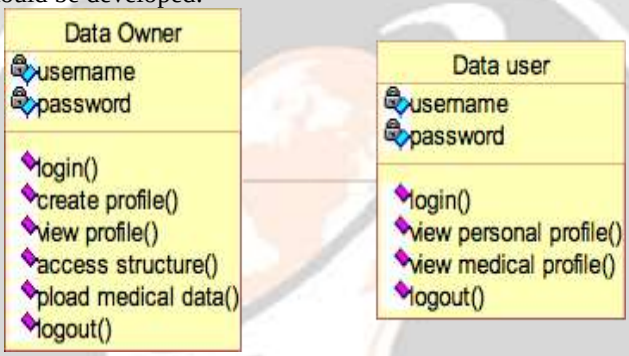

Fig. 5- Class Digram

3.4 USE CASE DIAGRAM:

A use case diagram is a behavioral diagram defined and created from a Use-case analysis. Its purpose is to represent a graphical overview of the functionality provided by a system in terms of actors and any dependencies. The main purpose of a use case diagram is to show how system functions are performed for which actor. Roles of the actors in the system can be depicted as below.

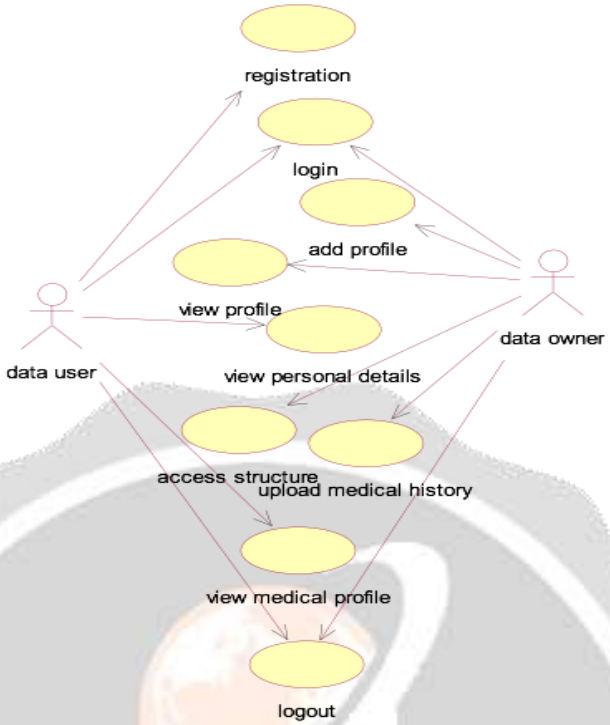

Fig. 6- Use Case Diagram

3.5 COLLOBORATION DIAGRAM:

In collaboration diagram the call sequence of methods is represented by numbering technique as shown be- low. The number indicates the way in which the methods are called after one another. Same management system is used for describing the collaboration diagram.

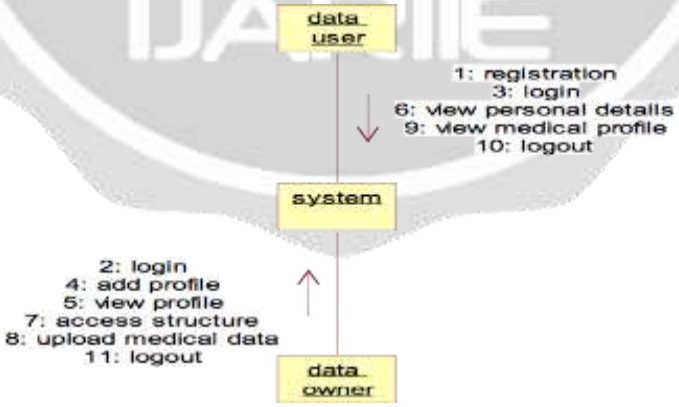

Fig.7-Collabration Diagram

4 RESULT

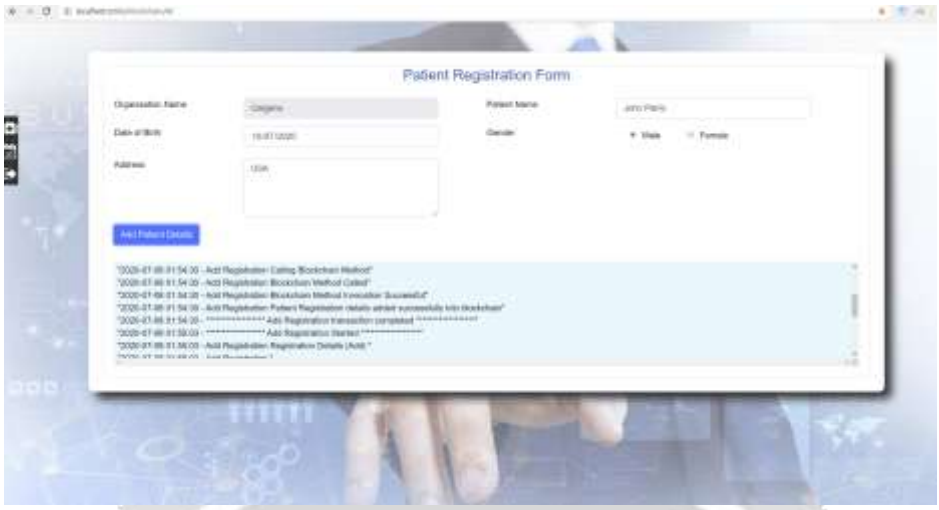

Fig. 8-Patient Registration form

Fig. 9-Event Registration form

It is the first page when all user can login with there username and password also new user can register in system. Fig. 9 shows registration form where user have to register first to use this application.

Fig. 10-Auditor Login

In the Fig.11 bar chart shows the comparing results of Views and Recommends ofdifferent Patient. It is used for immediate data comparison.

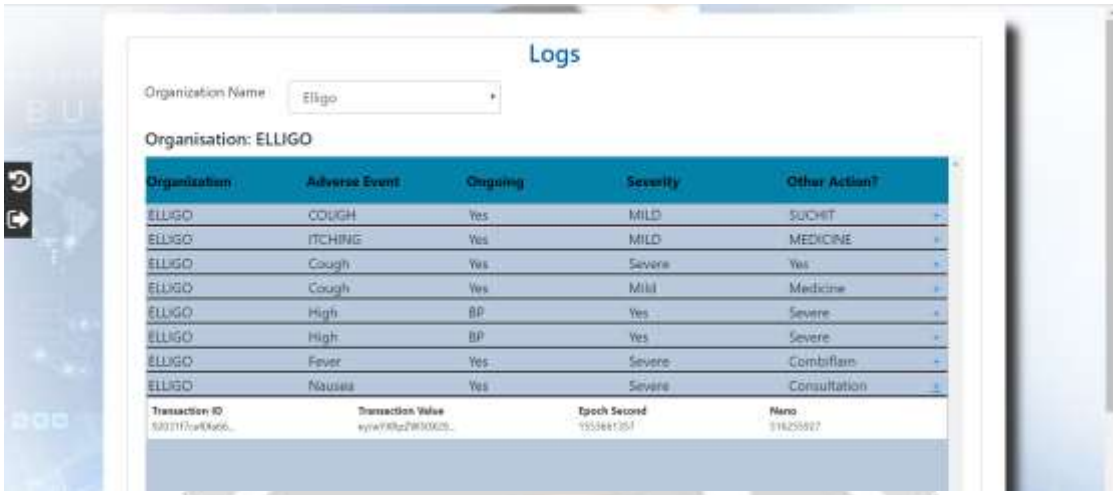

Fig 11-Log Fetched from Blockchain

5. CONCLUSION AND FUTURE SCOPE

In this paper discussed about permissioned and permissionless Blockchains with their architecture, and also how they could be implemented in healthcare. In addition, I also try to discussed related (about) security and privacy challenges, and how the use of Blockchains could come to an end due to quantum computers. Moreover, the paper suggested possible solutions for the a forementioned problems. scenario we can now consider in addition to health, health records are also wealth. So it is more important to keep our health records safe. The world has started moving towards patient-driven interoperability where patients provide the on- demand access to their health records.

In this model, the patient is considered as the sole owner to his health records who would decide on sharing what data and with whom. 200 health executives were interviewed by IBM's Institute for Business Value Blockchain, of which 16 percent of people are ready to deploy commercial Blockchain. As discussed above, Blockchain does not just help in decentralizing the data, it also gives the real-time data access, keeps the data confidential, handles high volumes of data efficiently, and also authenticate and authorize the data.

6. REFERENCES

[1]A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aladhari andM. Ayyash, "*Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications*," IEEE Communication Surveys & Tutorials, vol. 17, no. 4, pp. 2347- 2376, 2015.

[2]Department of Health, "*Whole System Demonstrator Programme Headline Findings – December 2011*," United Kingdom Department of Health, 2011.

[3]Zyskind, Guy, and Oz Nathan. "*Decenterilized privacy: Using blockchain to protect personal data.*" Proceedings of the 2015 IEEE Security and Privacy Workshop (SPW) May 21-21,2015, San Jose, California, USA. pp 180-184.

[4]S. Nakamoto, "*Bitcoin: A peer-to-peer electronic cash system,",* White paper, Oct. 2008, available at https://bitcoin.org/bitcoin.pdf.

[5] N. Zhumabekuly Aitzhan; D. Svetinovic, "*Security and Privacy in Decentralize Energy Trading through Multi-signatures, Blockchain and Anonymous Messagin Streams*," in IEEE Transactions on Dependable and Secure Computing , vol.PP, no.99, pp.1-1 doi: 10.1109/TDSC.2016.2616861.

[6]K. Christidis and M. Devetsikiotis, "*Blockchains and Smart Contracts for the Internet of Things*," in IEEE Access, vol. 4, no., pp. 2292-2303, 2016. doi: 10.1109/ACCESS.2016.2566339.

[7]A. Yasin and L. Liu, "*An Online Identity and Smart Contract Management System*," 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC),

[8] Atlanta,GA, 2016, pp. 192- 198. doi: 10.1109/COMPSAC.2016.2. A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "*Hawk: The Blockchain Model of Cryptography and Privacy- Preserving Smart Contracts*," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2016, pp. 839-858. doi: 10.1109/SP.2016.55.

[9]A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "*MedRec: Using Blockchain for Medical Data Access and Permission Management*," 2016 2nd International Conference on Open and Big Data (OBD), Vienna, 2016, pp. 25-30. doi: 10.1109/OBD.2016.11

[10]Y. Yuan and F. Y. Wang, "*Towards blockchain-based intelligent transportation systems,"* 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, 2016, pp. 2663-2668. doi: 10.1109/ITSC.2016.7795984.