Journal of Harbin Engineering University Vol 45 No. 1
ISSN: 1006-7043 January 2024

Block chain Technology Transforming Healthcare Industries: An Overview

Dr. Aditi Banerjee , Mr. Subhankar Banerjee
Assistant Professor, Bharati Vidyapeeth's Institute of Management Studies and Research.
Associate Director- Infrastructure &Smart Cities Advisory Langia
Anderson Co LLP

Abstract
Rising global costs and the uneven nature of the healthcare supply chain creates several challenges. The healthcare industry needs efficient solutions that can streamline operations and processes in a cost- effective manner. Leading healthcare players are exploring block chain technologies to achieve efficiencies and gain better control over their work process. In this paper, we present the current state of the subject and summarize the benefits and challenges of the disseminated organization and management of healthcare industries. Block chain is an emerging technology being applied for creating innovative solutions in various sectors, including healthcare. A Block chain network is used in the healthcare system to preserve and exchange patient data through hospitals, diagnostic laboratories, pharmacy firms, and physicians. Block chain applications can accurately identify severe mistakes and even dangerous ones in the healthcare field. Thus, it can improve the performance, security, and transparency of sharing medical data in the health care system. This technology is helpful to medical institutions to gain insight and enhance the analysis of medical records. In this paper, we studied Block chain technology and its significant benefits in healthcare. Various Capabilities, Enablers, and Unified Work-Flow Process of Block chain Technology to support healthcare globally are discussed diagrammatically. Finally, the paper tries to develop two different models which can improvise the workflow of Healthcare industries with the applications of Block chain Technology.

Keywords: Healthcare, Opportunities, Challenges, Block chain, Transformation

Introduction:

The world of technology and more specifically the information and communication technology has developed at an enormous speed in recent decades. We have travelled from a room sized computing machine to microchip sized super computers capable of handling and processing loads of data in milliseconds and microseconds. However, the Covid 19 pandemic has taught a haunting lesson that the human race might have developed itself in the technology domain but in the healthcare domain we need more and more technological intervention not only for the prevention of such pandemic but also taking precaution at a massive level to protect the humankind from any such pandemic in future. Blockchain is one of those emerging technology which if explored at the optimum level can revolutionize the healthcare sector and service landscape globally.

Before we dive in to details, first of all we need to understand "What Blockchain is", "Why Blockchain is important', and "work process of Blockchain ".

Blockchain Technology

In very simple words, Blockchain is a decentralized, distributed and public digital ledger that can record any transactions and/or track any tangible or intangible assets, thus building trust in a business workflow. It records every transaction on multiple systems in a "Block" structure that is verified and confirmed by every node in the network and linking every such "Block" to its preceding "Block", forming a long "Chain of Blocks" in which no particular "Block" or "Record" can be changed and/or distorted without altering other "Blocks" linked with that "Block", hence making it impossible to change any particular "Block" without changing the entire chain of blocks.

Due to the "Decentralization" of the architecture no single node or person has absolute access to the system information and thus gives a Blockchain the attribute that any decision taken is made across various nodes, where each node decides separately, which ultimately accumulated as the behavior of the entire system. As there are many nodes working on the same network on real time and the capability of each node is combined

together, the decentralized architecture provides a humongous amount of computing capability. At the same time the "Distribution" all parts of the system is spread across different physical locations across multiple nodes, hence building the system more secure and impregnable. Combination of these two characteristics provides the nodes to communicate and coordinate through secure messaging channels and also empowering to decide the decision making either in a centralized or decentralized manner. The final architecture comes up with various advantages like –

- The decentralization provides more control to users.
- More reliable and stable as no single entity has control over the entire network, thus no single point of failure. If one node fails, it won't have the capacity to fail the entire system.
- As there are multiple nodes working in the system simultaneously and every block is chained to its preceding and following block, this makes the architecture more secure as hackers need to attack multiple nodes simultaneously placed in different network and also different zones.
- Increased computation power, enhanced speed and flexibility coupled with high scalability of the system makes the entire system more proficient of managing high volume of unremitting critical data load.

Importance of Block chain in Healthcare Industry

Traditional database system faces several challenges regarding data security and management. In a traditional architecture the database could be viewed as a centralized ledger where the Administrator of that database or ledger has the highest level of access and capacity. The administrator is the sole authority to provide any or all of the four types of permissions to any user in the database. The four types are Create, Read, Update and Delete (collectively termed CRUD) and the user with "Update" and/or "Delete" permission has the access to permanently change or overwrite a data, resulting to data manipulation and/or data loss, which in turn could make the sanctity of the data questionable and thus creating any or all of the issues related to legal, technical, financial and business. Moreover, if not an expensive solution of "Real-time backup" of the database is maintained, the architecture also has a disadvantage of single point of failure.

On the other hand, when it comes to the storing of data Blockchain works completely differently. A typical Blockchain ledger is made up of multiple decentralized nodes working together from different zones. There is no centralized Administrator of the database, as each node participating in the ledger is an administrator. Every node verifies any new operation in the ledger. A new block of data can only be added in the existing chain if all the nodes in the structure verify the addition and make a consensus on the same, which in turn provide assurance about the security of the data and makes the structure difficult to corrupt. Out of many available and developed, "Proof-ofWork" is one of the most popular consensus algorithms. This algorithm requires each node to solve intricate mathematical problems to authenticate any transactions in the ledger. On top of that every transaction in a Blockchain ledger is cryptographically signed using complex cryptographic algorithms to ensure that each transaction is valid and originated from a valid source. Here it should also be mentioned that the blockchain architecture is an "Add Only" data structure. Any node can only add data in the existing data chain as an additional block. Once added, the data is permanently stored and cannot be altered in future. Therefore, any node can run either a READ operation to make a query and retrieve information from the ledger or a WRITE operation to add data on to the ledger. This structure could be viewed as a chain of blocks that is impermeable to tampering as each block is bind with a cryptographic hash of the block preceding it. Thus make it impossible to change the data in any block without changing the previous block after a block is successfully added to the blockchain and any attempt of doing that would actually quash the entire chain.

Workflow of Blockchain

The technology owes its name from the structure it uses to store its data in the ledger – data stored in a "Block" structure and each block is coupled with other blocks to form a "Chain" of blocks. Each of these blocks contains three main components – A Hash key (unique identification number), Timestamp and the Hash key of the previous block. This "Hash key of the Previous Block" actually makes the entire chain immutable by making the data stored in any particular block from being manipulated or tampered. The four most important parts of the Blockchain concepts are –

a. **A Shared ledger**, which is an "addonly" distributed structure of record shared over a network, in which any transaction can only be recorded only once as a block and once successfully recorded it is impossible to edit or delete that data block without harming the entire

chain of blocks, hence eliminating the threat of data manipulation.

b. **Authorization**, to guarantee that each and every transaction is verified and authenticated by all the nodes in the network and also the data stored in that transactional block is secured.

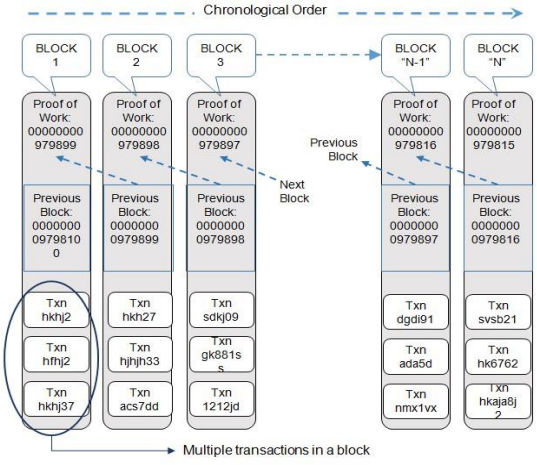
c. **Smart contracts**, which could be considered as the list of rules that every transaction is ought to follow. This is a part of the blockchain itself and is triggered automatically whenever a transaction takes place in the Blockchain.

d. **Consensus** is the algorithm via which all nodes in the network come to an agreement to the verified transaction. Blockchain technology uses various consensus algorithms, like Proof-of-Work (PoW), Proof of Stake (PoS), Multisignature, Proof of Authority (PoA), Byzantine Fault Tolerance (BFT), Direct Acyclic Graph (DAG), etc.

Before we dive deeper in to the aspect of how a Blockchain works, we also need to have an overview of the main stakeholders in any Blockchain network and the character they play in the network –

a. **Nodes / Participants** – These are in general authorized and verified business users of the blockchain network who have permissions to carry out transactions with other nodes / participants in the network.

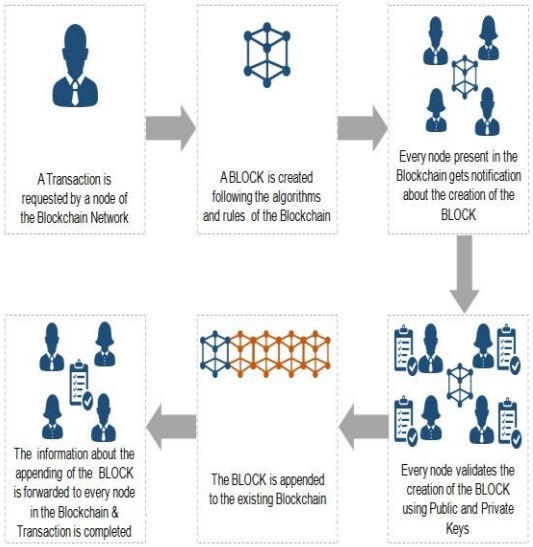
b. **Regulatory Members** – They could be considered as the guardians of the Blockchain,



who have the permissions to administer every transactions taking place in the network.

c. **Network Operators** – They are individuals with authorization and right to define, create, manage, and monitor the blockchain network.

d. **Certifying Members** – These are persons, who are authorized to provide and manage various types of legal, technical, operational, regulatory and other essential certificates to run a blockchain. Now let us look in to the process flow step-by-step to understand how a transaction is initiated, validated and finally recorded in a shared ledger of a Blockchain –



Step 1 – First, a transaction is requested from one of the nodes in the blockchain network. The node making the request has to be an authentic and authorized business user of the blockchain. **Step 2** – After a transaction is requested in the blockchain network, a Block is created representing that transaction. The Block contains the details about the transaction and is created as per the algorithms and regulations set up for the blockchain.

Step 3 – Once the Block is created, every node in the blockchain network receives a notification about the newly created Block and gets details of the transaction.

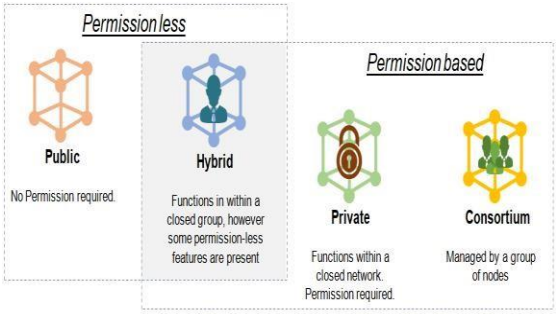
Step 4 – After receiving the notification each and every node in the network needs to "validate" that transaction and only then the transaction will be considered as an authentic transaction. **Step 5** – Once, every node has validated the transaction the newly created Block is appended in the existing chain and becomes an immutable data block of that blockchain which is connected with Hash of the previous block. **Step 6** – As the new Block is appended in the blockchain, every node receives a notification about the successful completion of the operation and the transaction is considered completed.

Types of Blockchain

Every blockchain network is designed and developed keeping in mind the purposes and requirements for the blockchain. Different purposes have different

requirements and different requirements create different models as per their necessities. However, from architectural point currently there are mainly four types of blockchain network is available – Public, Private (or Managed), Hybrid and Consortium. Each type has its own characteristics, advantages, disadvantages and usage.

Public Blockchain – This is a distributed ledger



system where no permission is required and there is no restriction to join the network. Any user who has joined this type of blockchain is approved of accessing any records in the ledger, validate transactions and conduct other legitimate activities. In this model each user keeps a copy of the ledger.

a. Private Blockchain – Contrary to the "Public" model, this type of blockchain model functions within a closed network of nodes where only selected users are authorized to use that blockchain network.

b. Hybrid Blockchain – As the name suggests, this architecture is a mix and match of the features required from both the permission-based as well as permission-less systems. It enables a group of people to construct a private system alongside a public one, thus allowing them to choose who has access to certain Blockchain data and what data is made public. However in a hybrid model, transactions and information are not made public, but if required, the same can be validated by granting access via a smart contract.

c. Consortium Blockchain – In this variant of blockchain, a group of organizations actually manages the network and control the consensus processes. However at the same time it as there is no central authority and the blockchain is controlled by numerous organizations it retains a decentralized aspect despite not being accessible to many people.

Literature Review:

Blockchain technology has been exhaustively researched in the past few years. The fundamental concept of the blockchain technology gives a basis for cooperation between unknown and untrustworthy things, while also corroborating the disseminated features of mobile (smart health) devices, lacking the need of a central security and authentication authority, as in the current cloud computing architectures [13]. The key characteristics of blockchain technology includes decentralized control, data transparency and auditability, distributed information, and security from malicious actors [6]. A report by MIT Media Lab [24] presented about security and privacy aspects of data and personal information handling underlining all of the blockchain technology implementations. It is the value of the secure processing of data–in the sense that it cannot be manipulated.

Gordon and Catalini [20] published a review on healthcare blockchain where they concluded their discussion on how blockchain technology can enable patient-centric control of healthcare data sharing over institution centric control. In their study they examined how blockchain technology transforms the healthcare sector by enabling digital access rights, patient identification across the network, handling a large volume of healthcare data and data immutability.

In healthcare supply chain management, the blockchain technology transactions is particularly key monitoring technology for tapping into the whole process of drugs and medical products movement [7].Since all transactions are recorded onto the ledger, and every node in the blockchain maintains a record of the transaction, it is easy to verify the origin of the drug, the vendor and the distributor instantly. Furthermore, the distributed ledger of the blockchain allows healthcare officials and physician to check and authenticate the credentials of suppliers [8].

. In 2009, U.S. Health Information Technology for Economic and Clinical Health (HITECH) Act reserved approximately 36.5 billion dollars to invest in health organizations to use EHR systems instead of the traditional methods to manage data [2]. Nowadays, the EHR market is highly valued, which may be counted in the figure of tens of billions of dollars [1]. However, sharing health data needs a secure and trusted infrastructure as there exists many risks related to privacy, security, and interoperability. Firstly, health data have huge privacy-sensitivity; particularly as more and more data is being stored on the cloud. Therefore, the challenges of revelation and leakage of confidential data are increasing. Secondly, the centralized architectures are widely used in the current systems as well as in the security mechanisms. Hence, it is challenging to effectively integrate interoperability among healthcare

systems, which are distributed in deployments. In addition, it is also a major challenge that users have less access to the private health data [3].

Recently, blockchain has been adopted by several government, private, and public-private partnered projects [14]. Blockchain's potential benefits in the field of healthcare were witnessed when the US Food and Drug Administration (FDA) [15]. Blockchain allows data collection from various sources and saves that data in the transaction audit log, which ultimately helps in keeping track of accountability and transparency of data at the time of data exchange. It is believed by FDA and IBM that blockchain has the capability to support data exchange collected from various sources with the consensus of patients and the terms mutually agreed on [14].

Blockchain can be a solution to these issues that may lead to solving a general problem of privacy and authentication. It also supports data auditing and time-stamping that could help patients to identify modifications in data with respect to time as well as identity of the person who modified it. In a blockchain scenario, patients can permit third parties to access data, however, third parties cannot store it. To conclude, blockchain-based solutions are higher-ranked than existing traditional systems. Blockchain helps marketers to maintain an overview of the products used in medicine. Health and pharmaceuticals will get rid of counterfeit medications using Blockchain technologies, enabling tracing of all these medicines. It helps discover the cause of falsification. Blockchain can guarantee the confidentiality of patient records; when medical history is developed, Blockchain can also store it, and this record cannot be modified. [4, 5].

The Blockchain enhances healthcare organisations to provide adequate patient care and highquality health facilities. Health Information Exchange is another timeconsuming and repetitive process that leads to high health industry costs, quickly sorted out using this technology. Using Blockchain technology, citizens may take part in health study programs. In addition, better research and shared data on public wellbeing will enhance treatment for different communities. A centralised database is used to manage the entire healthcare system and organisations [9-10].

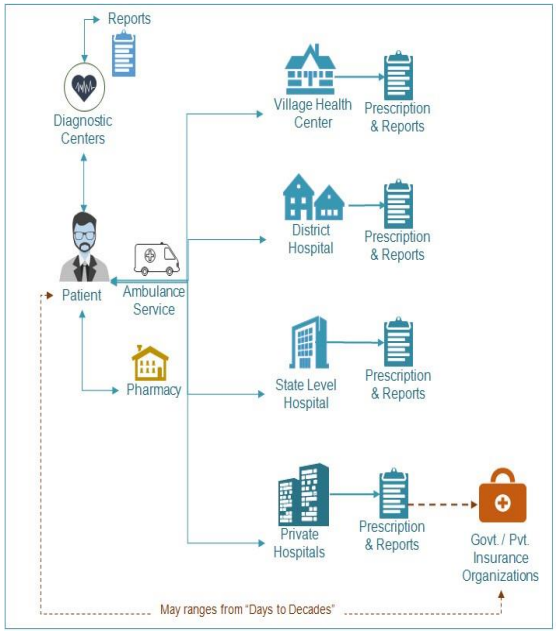
Until now, the most significant problems faced are data protection, sharing, and interoperability in population health management. This particular problem is reliable by using Blockchain. This technology enhances security, data exchange, interoperability, integrity, and real-time updating and access when correctly implemented. There are also significant concerns about data protection, especially in the fields of personalised medicine and wearables. Patients and medical personnel require safe and straightforward means of recording, sending, and consulting data over networks without safety concerns; thus, Blockchain technology is implemented to resolve these issues [11,12]. The benefit for patients is that their medical histories are protected more confidently and that their diagnostic accuracy improves chances of further care [16,17].

In the processing of their health records, patients will now have a better voice. It will be allowed to exchange data as partners of the Blockchain network, thereby ensuring further privacy and control. Blockchain's pledge has widespread consequences for health care stakeholders. Disparate networks are likely to interact to provide insights and help evaluate treatment's importance based on this technology. An electronic medical records Blockchain network around the country will increase efficiencies and promote improved patient health results in the long run. In particular, Blockchain is a mutual, unchanging record of transactions made from connected transaction blocks and held in a digital booklet [18, 19]. Medical details like patient life, medical equipment logs, or medical products' temperatures can be recorded during the shipping, following the medical field.

Blockchain can become a fundamental aspect of the administration of consents to healthcare that facilitates knowledge exchange. Patients can now link to other hospitals and automatically receive their medical information via Blockchain technology [23]. Blockchain will significantly minimize financial failures and also avoid theft and the illicit transferring of records. It can solve problems of changing results and snooping data. It allows the transfer of permanent time-stamped clinical trial reports and results, thus reducing scam and mistake occurrences in clinical trials. The health industry is primarily responsible for adopting Blockchain technologies [21, 22].

Current Healthcare Scenario: Challenges & Issues

- No standard and secured process of sharing information leads to



○ data duplication at various levels human errors causing severe damage ○ data inconsistencies leading to confusion ○ unnecessary Costs for repetative diagonostic tests

- Middlemen take advantages of lack of standardized information that leads to fraudulent activities.
- No privacy and security of medical data • No consensus from the patient or providers on Data Sharing
- No scope for Healthcare Data Exchange & Interoperability
- No shared, trusted, verified & real-time data on Medical Transportation and available facilities.
- No scope for Clinical Trails & Population / Demographic Health Research
- Data in silos are not irrevocable or immutable and open to tamper
- No scope for the Govt. to verify Drug Supply Chain Integrity & Remote Auditing
- No Trust Network across various organizations (Health Centers & Hospitals) leading to repetition, duplication and scope for errors. No "Book-Keeping" of data exchange.
- Cost per Transaction for the patient is very high and also lacks standardization
- Master Patient Index (MPI) challenges arise from the need to synchronize multiple patient identifiers between systems while securing patient privacy.
- Varying Data Standards reduce interoperability because records are not compatible between systems.
- No access to Population Health Data due to unavailability of a source of integrated records. • Inconsistent Rules and Permissions inhibit the right health organization from accessing the right patient data at the right time.

Gap Analysis:

Through our Literature Review and research analysis we have gone through during our study has realised the different problems and challenges faced by healthcare industries in India and also realiised how the application of Blockchain Technology can improvise the system. But in our research we have tried to develop two different models through which we can make an improved Healthcare industries.

Objective of the Study:

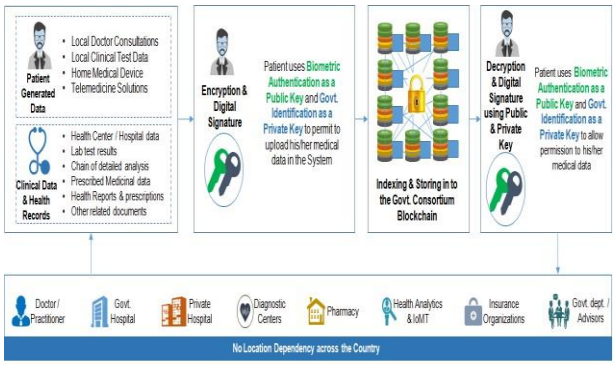
The objective of the study is providing a solution to the Healthcare sector with a Model which can improve the Workflow of healthcare industries. **Expected Changes in Healthcare Industry in adoption of Blockchain Technology**

- It will help the focus to be shifted more efficiently towards management of data that would increase the potential to connect disparate systems and increase the accuracy of Electronic Health Records.
- Blockchain would make Clinical data, Medical supply chain, Transparency framewok and Risk assesment and management more trust worthy, easily available and efficient.
- The adoption of this teachnology will support access control, data sharing and managing of an audit trail of medical activities securely under a consensus algorithm.
- It can help to accomplish Provider Credentials, Medical Billing, Smart Contracting, Clinical Record exchange, Clinical Trials, and AntiCounterfeiting Drugs.
- Blockchain-based healthcare systems would enhance security and reliability of patients' sensitive data since patients would have control over their healthcare records.
- This could also be used in a scenario where multiple parties, who do not trust each other need to interact and exchange common data, but would not like

to take the burden of a considerable additional cost of involving a Trusted Third Party (TTP).

- The immutability of the data stored in the Blockchain will be the most helpful attribute to check malpractices and counterfeiting of data in the healthcare system.

Proposed Solution : Workflow



- Data Security, Integrity and Accessibility –

○ Stores different types of health data (e.g. Image, Lab Reports) ○ Maintains structured & standardized data format

○ Data is encrypted & secured through digital / biometric signature

○ Consists a complete indexed chronologically timestamped health history with unique identification & an encrypted Hash value to the data

○ Data is under exclusive control of the patient for accessing and/or sharing

Model 1 Overview:

- Use existing protocols or Direct Messaging to send Clinical data to a Blockchainbased PHR, which is equipped to receive data according to the standards.
- The Blockchain-based PHR would handle these communication protocols and configured to receive documents from various sources.

Process

1. Stakeholders connect to the system & transfers data.
2. The **Outer wall application** receives and transfer the data to the **Inner wall application**
3. The **Inner wall application** standardizes the received document as per the Blockchain architecture along with metadata and transfer the same to the Blockchain Solution.
4. The Blockchain solution commits this as a transaction to the Blockchain and uses consensus algorithm to determine the transaction's validity. Only when a quorum of nodes agrees to the change, it is permanently committed to the public ledger.
5. The Stakeholders connects to the Blockchain and download all documents as required. The documents are decrypted using the patient's private key.

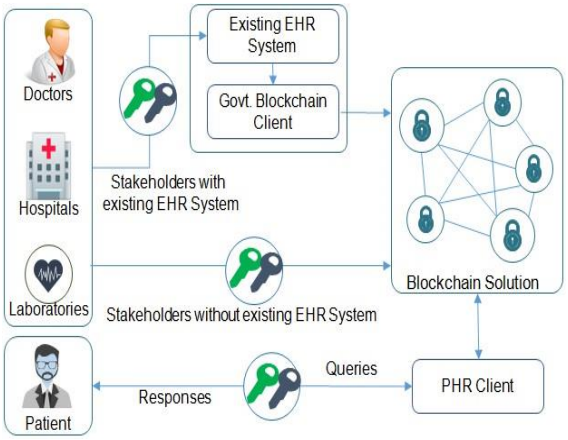
Challenge:

- Blockchain-based system is conceived as a simple distributed electronic transaction ledger, such integrated functionalities make the system heavy.

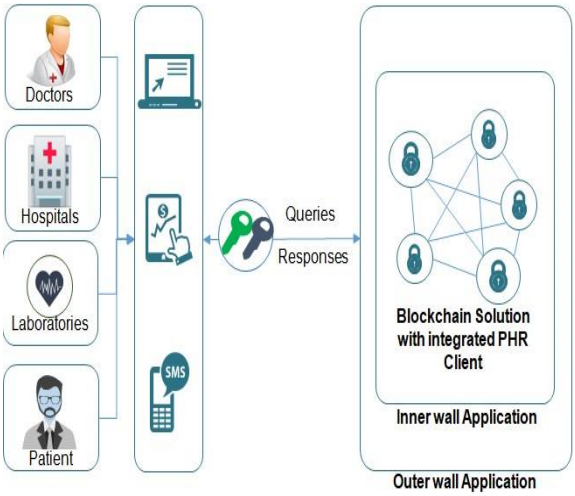
Model 2 Overview:

- Govt. develops a **Blockchain client** and guide the stakeholders who are currently storing their patients' data in an EHR system to use that **Blockchain client** to communicate clinical information directly to the Blockchain-based PHR.
-

Process



1. Stakeholders with existing EHR



System save data locally, prepare a standardized version and transfer it to the built-in Blockchain client.

2. The Blockchain client encrypts the document using the patient's public key and transmits the same to the Blockchain in the defined format.

3. The standardized document, along with metadata about the document's source and subject, is committed as a transaction to the Blockchain. The nodes of the Blockchain network use a consensus algorithm to determine the transaction's validity, and when a quorum of nodes agrees to the change, it is permanently committed to the public ledger.

4. The PHR client connects to the Blockchain and downloads all documents for the patient. The documents are decrypted using the patient's private key.

5. The patient can view and share the documents with other providers.

• Challenge:

This approach requires effort and cooperation on the part of all the Stakeholders and is unlikely to occur without regulation or incentive. **Expected Outcomes of the proposed workflow and model :**

○ Healthcare data exchange Provide access to historic and real-time Clinical Data on Blockchain

 Identity management with predefined user access rules for P2P networking

 Store genomics and user generated data securely, with access control

 Maintain universal health records and identities

○ Info Security & Internet of Medical Things (IoMT)

 Encryption and permanent ledger of patient-generated health data

 Secure Medical device data integration enable remote/home care

 Unique identifiers for medical devices or assets on distributed ledger system to automate maintenance and management ○ Drug Supply Chain Integrity & Remote Auditing

 Drug supply chain provenance at individual product/drug level

 Blockchain-based remote process auditing with verifiable source of truth

 More Integrated and Improved pharma supply chain finance

 More visibility for marketing efforts and medication adherence programs ○ Clinical Trails & Population Health Research

 Manage Identity and assets transactions on Blockchain

 Reduce outcome switching, data snooping, and selective reporting

 Better and faster regulatory compliance and approvals

 Bilateral interactions and communication with all stakeholders

Conclusion:

There are advanced applications of Blockchain in healthcare due to inherent encryption and decentralization. It enhances the security of patients' electronic medical records, promotes the monetization of health information, improves interoperability among healthcare organizations, and helps fake battle medicines. The Blockchain potential in healthcare depends significantly on the adoption of associated advanced technologies in the ecosystem. It includes system tracking, healthcare insurance, medicines tracing, and clinical trials. Hospitals can chart their services using a Blockchain framework. Blockchain technology can well be used to improve patient history management, especially tracking and the insurance mediation process, thereby accelerate clinical actions with optimized data maintenance. Overall, this technology would significantly enhance and eventually revolutionize how patients and physicians treat and use clinical records and improve healthcare services. We have tried to develop Models in our research paper through which blockchain-based solutions can overcome different security issues in an efficient, distributive, and scalable way. In future, we aim to expand our study to an in-depth analysis of the authentication mechanisms to design an efficient blockchainbased identity authentication Model.

References:

[1] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, Provchain: A blockchain-based data

provenance architecture in cloud environment with enhanced privacy and availability, in: 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), IEEE, 2017, pp. 468–477.

[2] R. O. Jr., The Machinery Behind Health-Care Reform, https://www.washingtonpost.com/wpdyn/content/article/2009/05/15/ AR2009051503667.html, [Online; accessed 27-May-2020] (2020).

[3] L. J. Kish, E. J. Topol, Unpatients—why patients should own their medical data, Nature biotechnology 33 (9) (2015) 921.

[4] A. Ali, F. A. Khan, A broadcast-based key agreement scheme using set reconciliation for wireless body area networks, Journal of medical systems 38 (5) (2014) 33.

[5] F. A. Khan, A. Gumaei, A. Derhab, A. Hussain, A novel two-stage deep learning model for efficient network intrusion detection, IEEE Access 7 (2019) 30373–30385.

[6] U. Khalid, M. Asim, T. Baker, P. C. Hung, M. A. Tariq, L. Rafferty, A decentralized lightweight blockchain-based authentication mechanism for iot systems, Cluster Computing (2020) 1–21.

[7] N. Tariq, M. Asim, Z. Maamar, M. Z. Farooqi, N. Faci, T. Baker, A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered iot, Journal of Parallel and Distributed Computing 134 (2019) 198– 206.

[8] N. Abbas, M. Asim, N. Tariq, T. Baker, S. Abbas, A Mechanism for Securing IoT-enabled Applications at the Fog Layer, Journal of Sensor and Actuator Networks 8 (1) (2019).

[9] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, I. Ghafir, The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey, Sensors 19 (8) (2019) 1788.

[10] N. Tariq, M. Asim, F. A. Khan, Securing scadabased critical infrastructures: Challenges and open issues, Procedia Computer Science 155 (2019) 612–617.

[11] F. A. Khan, N. A. H. Haldar, A. Ali, M. Iftikhar, T. A. Zia, A. Y. Zomaya, A continuous change detection mechanism to identify anomalies in ecg signals for wban-based healthcare environments, IEEE Access 5 (2017) 13531– 13544.

[12] H. Wang, K. Li, K. Ota, J. Shen, Remote data integrity checking and sharing in cloud-based health internet of things, IEICE TRANSACTIONS on Information and Systems 99 (8) (2016) 1966–1973.

[13] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, J. Wang, Untangling blockchain: A data processing view of blockchain systems, IEEE Transactions on Knowledge and Data Engineering 30 (7) (2018) 1366–1385.

[14] N. Kshetri, Blockchain and electronic healthcare records [cybertrust], Computer 51 (12) (2018) 59–63.

[15] L. Mearian, IBM Watson, FDA to explore blockchain for secure patient data exchange, https://www.computerworld.com/article/3156504/ibm-watson-fda-to-exploreblockchain-for-secure-patient-data-exchange.html, [Online; accessed 28May2020] (2020).

[16] A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M. A. Ferrag, M. Mukherjee, F. A. Khan, Blockchain and random subspace learning-based ids for sdn-enabled industrial iot security, Sensors 19 (14) (2019) 3119.

[17] A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman, A case study for blockchain in healthcare:“medrec” prototype for electronic health records and medical research data, in: Proceedings of IEEE open & big data conference, Vol. 13, 2016, p. 13.

[18] HIPAA, The HIPAA Privacy Rule, https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html, [Online; accessed 28May-2020] (2020).

[19] L. A. Linn, M. B. Koo, Blockchain for health data and its potential use in health it and health care related research, in: ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST, 2016, pp. 1–10.

[20] M. Du, Q. Chen, J. Chen, X. Ma, An optimized consortium blockchain for medical information sharing, IEEE Transactions on Engineering Management (2020).

[21] A. Shahnaz, U. Qamar, A. Khalid, Using blockchain for electronic health records, IEEE Access 7 (2019 Oct 9) 147782¯147795.

[22] W.J. Gordon, C. Catalini, Blockchain technology for healthcare: facilitating The transition to patient-driven interoperability, Comput. Struct. Biotechnol. J. 16 (2018 Jan 1) 224¯230.

[23] A.A. Siyal, A.Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, G. Soursou, Applications of blockchain technology in medicine and healthcare: challenges and future perspectives,

Cryptography 3 (1) (2019 Mar) 3.

[24] Change 165 (2021 Apr 1) 120536.

[25] N. Tariq, A. Qamar, M. Asim, F.A. Khan, Blockchain and smart healthcare security: a survey, Procedia Computer Science 175 (2020 Jan 1) 615–620.