Dissertation Report

on

Blockchain: A Revolution in the Field of Health Care

Submitted in partial fulfillment of the

requirement for the award of the degree of

Bachelor of Technology in Computer Science Engineering

Under The Supervision of
Dr. S Rakesk Kumar
Assistant Professor

Submitted By

ISHAAN VIJAY VERMA
19SCSE1010790
NAMIT GOEL
19SCSE1010198

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
GALGOTIAS UNIVERSITY, GREATER NOIDA
INDIA
DECEMBER, 2021

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
GALGOTIAS UNIVERSITY, GREATER NOIDA

CANDIDATE'S DECLARATION

I/We hereby certify that the work which is being presented in the thesis/project/dissertation, entitled **"BLOCKCHAIN: A REVOLUTION IN THE FIELD OF HEALTH CARE"** in partial fulfillment of the requirements for the award of the Bachelor Of Technology in Computer Science Engineering submitted in the School of Computing Science and Engineering of Galgotias University, Greater Noida, is an original work carried out during the period of July, 2021 to December and Year, under the supervision of Dr. S Rakesh Kumar Assistant professor, Department of Computer Science and Engineering of School of Computing Science and Engineering , Galgotias University, Greater Noida.

The matter presented in the dissertation has not been submitted by me/us for the award of any other degree of this or any other place.

Ishaan Vijay Verma
19SCSE1010790
Namit Goel
19SCSE1010198

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Dr. S Rakesh Kumar
Assistant Professor

CERTIFICATE

The Final Dissertation Viva-Voce examination of Ishaan Vijay Verma: 19SCSE1010790 and Namit Goel: 19SCSE1010198 has been held on _____ and his/her work is recommended for the award of Bachelor of Technology in Computer Science Engineering.

Signature of Examiner(s) **Signature of Supervisor(s)**

Signature of Project Coordinator **Signature of Dean**

Date: December, 2021
Place: Greater Noida

Acknowledgement

A lot of writing was inspected on blockchain based activities identified with the clinical business wherein a portion of the work centers basically around the information stockpiling perspective. As per the writing audit about existing programming stages, functionalities, systems, and innovations that have been utilized previously, the accompanying significant contemplations have been recognized and summed up in Figure 1.

Abstract

HRE(Healthcare Records Exchange) system, is meant to fulfill the desired needs according to the requirements of the healthcare system using blockchain technology. Blockchain is a decentralized database or sometimes called a ledger. A database with continuously growing records or lists which are linked to another block and secured using cryptography. Since the database is decentralized, P2P computing or networking is used, it is best for the execution of sensitive data like records of a patient in a hospital. It is a distributed application architecture that partitions the task between peers to complete the in a better flow. Here all the peers are equally privileged equipotent participants in the application. The form peer to peer or network of nodes. A smart contract is a programmable contract with terms and conditions between the parties. Which is contained within the decentralized Blockchain network. In the coming time in the field of medical science the data will be compared with various other databases of the hospital in which the risk of a data breach is higher using smart contracts and Blockchain this risk can be minimized as Blockchain technology is one of the most secure methods to secure the data with minimum requirements.

Contents

List of Table

List of Figures

Acronyms

HRE	Healthcare Record Exchange
P2P	Peer-to-Peer
EOA	Externally Owned Accounts
ECDSA	Elliptic curve digital signature algorithm
SC	Smart Contracts
UI	User Interface
CLI	Command Line Interface
PII	Personally Identifiable Information
HIPAA	Health Insurance Portability and Accountability Act
ICT	Information Communication Technology
SCM	Supply Chain Management

CHAPTER-1 Introduction

1.1 Introduction

This year, humanity was hit by one of the biggest catastrophes of the last 100 years: the COVID-19 pandemic, which led to both human and economic losses. It led to a universal increase of patients in the hospitals. This means more data for the healthcare industry to deal with, resulting in the awareness of the BlockChain technology in health care as the ultimate solution for enhancing interoperability between blockchains. Blockchain is a decentralized database, also the most disruptive technology of the decade. This technology is being opted by many verticals such as healthcare, Medicines, Insurance, Smart Properties, Automobiles, and even the head of the countries. Blockchain interest and momentum are now extended in the field of healthcare and information management.

A. Blockchain Transaction Process

A Blockchain transaction can be defined as a small unit of a task that is stored in public records. These records are also known as blocks. These blocks are executed, implemented and stored in the blockchain for validation by all miners involved in the blockchain network. Each previous transaction can be reviewed at any time but cannot be updated. Blockchain is the underlying technology of Bitcoin, and it facilitates transactions that occur within a peer to peer global network in a decentralized fashion. That makes Bitcoin a borderless, censorship-resistant digital currency. In general, trust may be the main concern regarding traditional centralized systems, such as banks, where people need to put their solemn confidence in the system. This is the sweet spot for public blockchain technology, in that it does not require any trust while handing over the ownership of digital assets from one peer to another. Blockchain is a trustless system that provides trust through the functions that propagate all the activities within the network. Security is another aspect to consider while initiating transactions. Blockchain mining and consensus mechanisms that rely heavily on a cryptographic hash function can address the security issues. For example, Bitcoin uses a 256 bits' secure hash algorithm known as SHA-256. Bitcoin can take any type of input, such as text, numbers, string or even a computer-generated file of any length, to produce 256 bits or the 64 characters output called hash. Given the same input, the converted hash output will always remain exactly

similar. However, a small change to the input will change the output completely, which is also called a one-way function, meaning that from the output, it is not feasible to calculate the input. One can only guess what the input was, and the odds of guessing it right are rather astronomical, in other words, it is secure.

The first step of the transaction process is to verify the identity of the sender, which means the transaction between the sender and the receiver is requested by the sender, and not by anyone else. The verification process with a simple example of a transaction. Let us assume Alice wants to pay 10 Bitcoins to Bob. Now, to send the money, Alice will broadcast a message with the information for the transaction in the blockchain network. To do this, Blockchain employs digital signatures (public and private keys). For the broadcast, Alice provides Bob's information, such as his public address and transaction amount, along with her public key and digital signature. Alice used her private key to make that digital signature. Transaction validation is carried out independently by all miners based on different criteria that we have discussed later in this section. Elliptic curve digital signature algorithm (ECDSA) is used by blockchain. This algorithm ensures that the funds can only be spent by their true possessors.

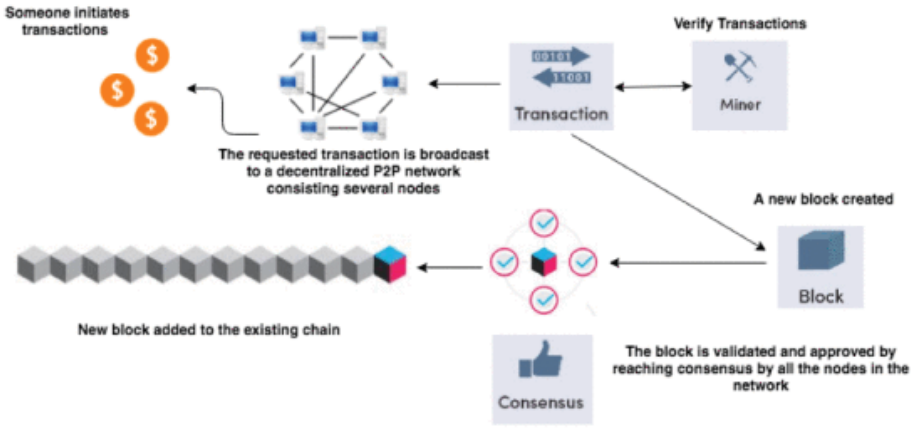

FIGURE 1: Functional diagram of a Blockchain network.

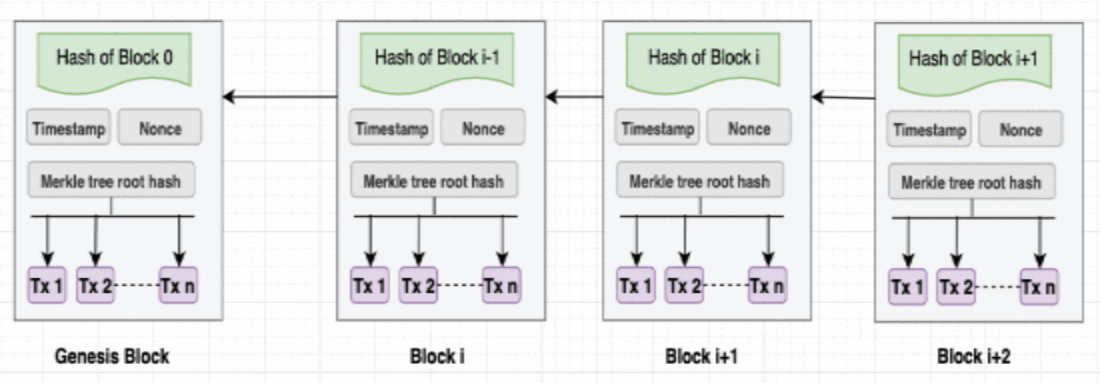

FIGURE 2: Block structure.

The signature in each transaction contains 256 bits, if anyone wants to fake this signature to make a fraudulent transaction, he or she has to guess 2^256 cases, which is infeasible and a waste of resources for a malicious peer/attacker. In addition to checking the validity of the sender, the verifier also has to check the validity of the transaction regarding whether the sender has enough money to send to the receiver, or not. It could be performed by looking at the ledger, which holds information about every past successful transaction.

Ethereum

EOA is needed to participate in the Ethereum network and interact with the blockchain using transactions, whereas CA represents a smart contract (SC). SC is a piece of code deployed in the blockchain's node and adds a layer of logic and computation to the trust infrastructure. Execution of an SC is initiated by a message embedded in the transactions.

In Ethereum, the transferable amount is known as ether. The denomination of ether is known as Wei. An Ethereum transaction has fields for transferring ether as well as messages to trigger smart contracts. Ethereum uses attributes similar to Bitcoin, for instance, previous block hash, nonce, and transaction details. Additionally, it uses some other fields such as fees limit, state of SC, and so on. For a simple ether transfer, the amount to transfer and the target address are specified, together with the fees, gas points, and the respective accounts. All the transactions generated will be validated by checking time stamp, nonce combination, and availability of sufficient fees for execution.

B. Block Structure

The Blockchain comprises a sequence of blocks, which stores the information of all the transactions, similar to a public ledger. These blocks are linked to each other via a reference hash that belongs to the previous block known as the parent block. The starting block is called the genesis block, which does not have any parent block. A block consists of the block header and the block body. The block header includes metadata such as block version, parent block hash, Merkle tree root hash, timestamp, nBits, and nonce as shown in Table 1 and Figure 2.

TABLE 1: Block Header Attributes

Header Attributes	Definition
Block Version	Indicates which set of block validation rules to follow.
Previous Block Hash	A 256-bit hash value that points to the previous block.
Merkle tree root	The hash value of all the transactions in the block.
Timestamps	Current timestamp as seconds since 1970-01-01T00:00 UTC.
nBits	Current hashing target in a compact format.
Nonce	A 4-byte field, which usually starts with 0 and increases for every hash calculation.

The block body is composed of a transaction counter and transactions. The transaction counter refers to how many transactions follow, and transactions represent the list of recorded transactions in the block. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions. A digital signature based on asymmetric cryptography is used in an untrustworthy environment such as the blockchain network. In this process, each participant in the network owns a private key and public key pair. The private key is used for signing or

encrypting the transaction while the public key is distributed throughout the network and is visible to everyone, which helps to decrypt the following transaction.

C. Characteristics of Blockchain

1) Decentralization

In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank). Therefore, decentralization requires trust, which is the main issue, along with lift resilience, availability and failover, where the decentralized peer-to-peer blockchain architecture could be a better solution. Unlike a centralized system, a transaction in the blockchain network can be conducted between any two peers (P2P) without the authentication by the central agency. In this manner, blockchain can reduce the trust concern by using various consensus procedures. Moreover, it can reduce the server costs (including the development cost and the operation cost) and mitigate the performance bottlenecks at the central server. In contrast, in many cases, blockchain has some tradeoffs. For example, PoW cases such as Bitcoin and Ethereum, the server and energy cost are orders of magnitude higher, while the performance are also several orders of magnitude lower.

2) Persistency

Blockchain provides the infrastructure by which truth can be measured and enables the producers as well as consumers to prove their data are authentic and not altered. For example, if a Blockchain consists of 10 blocks, then block no. 10 contains the hash of the previous subsequent block, and to create a new block, the information of the current block is used. Therefore, all the blocks are linked and connected with each other in the existing chain. Even the transactions are related to the prior transaction. Now, a simple update on any transaction will significantly change the hash of the block. If someone wants to modify any information, he has to change all the previous block's hash data which is considered an astronomically difficult task considering the amount of work that needs to be done. In addition, after generating a block by a miner, it is confirmed by other users in the network. Hence, any manipulation or falsification of data will be detected by the network. For this reason, blockchain is almost tamper proof and considered as an immutable distributed ledger.

3) Anonymity

It is possible to interact with the blockchain network with a randomly generated address. A user can have many addresses within a Blockchain network to avoid the exposure of his identity. As it is a decentralized system, no central authority is monitoring or recording users' private information. Blockchain provides a certain amount of anonymity through its trustless environment.

4) Auditability

All the transactions that occur in a blockchain network are recorded by a digital distributed ledger and validated by a digital timestamp. As a result, it is possible to audit and trace previous records by accessing any node in the network. For example, all the transactions could be traced iteratively in Bitcoin which facilitates auditability and transparency of the data state in the blockchain. However, by tumbling money through many accounts, it becomes very hard to trace the money to its origin.

Applications of blockchain:

Blockchain technology can be used in diverse sets of applications. It is important to understand that bitcoin is not equal to blockchain; instead, it is one of the most successful applications of blockchain technology. Bitcoin is a cryptographic digital currency, which is transacted over an open, public and anonymous blockchain network. However, experts claim that this technology can be implemented for finding solutions for different domains, such as healthcare, voting, identity management, governance, supply chain, energy resources and so on. Furthermore, some visionaries also predict that blockchain might influence the digital realm similar to the internet. When the internet first came along, we had no idea how it would forever change our lives. From smart phones and text messages to streaming movies and video conferences with loved ones, as well as for attending meetings or interviews, no one knew the ways the world would change with the invention of the Internet. We are currently in the early phases of blockchain and there is much potential yet to be unlocked. Figure 3. represents some of the application domains of the blockchain proposed by various experts. In this section, we have discussed some use case areas of blockchain suggested by researchers around the globe.

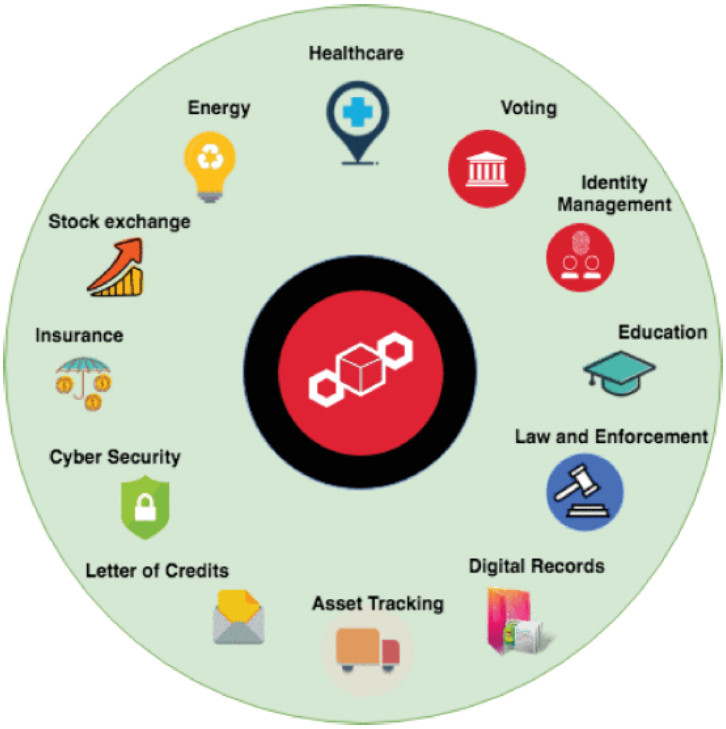

FIGURE 3: Application domains of Blockchain technology.

BlockChain in Healthcare

Distributed ledger technology possesses the potential to transform health services. Blockchain can be used for the traceability of drugs and patient data management. Drug counterfeiting is a major problem in the pharmaceutical industry. Reports from the Health Research Funding organization revealed that 10% to 30% of the drugs sold in developing countries involve counterfeit. It is estimated by the WHO that 16% of counterfeit drugs have the wrong ingredients, while 17% contain an imprecise level of essential ingredients. Therefore, these drugs can put a patient's life in danger as they will not treat the diseases, rather can trigger secondary effects that can lead to death. From an economic point of view, drug counterfeiting is responsible for an annual loss of 10.2 billion euros for European pharmaceutical organizations. Blockchain can be a solution to address this issue because all the transactions added to the distributed ledger are immutable and digitally timestamped, which makes it possible to track a product and make the information tamper-proof.

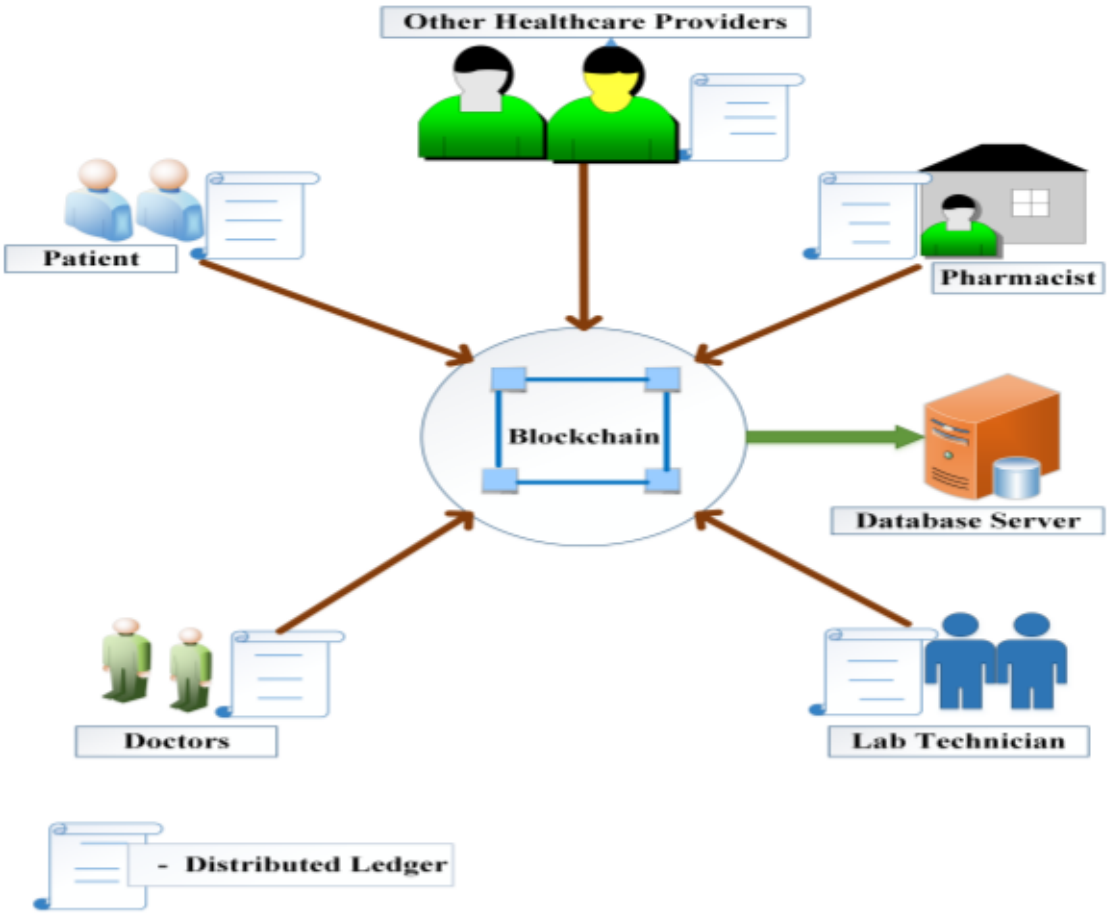

FIGURE 4: Block utilization in various healthcare applications

Managing patient data integrity is one of the major concerns for the healthcare industry. Each patient has unique physical variability, therefore a treatment strategy for a common disease varies depending upon circumstances. Hence, for providing personalized treatment, it is necessary to access the complete medical history of an individual patient. However, medical data is sensitive and requires a secured sharing platform. The existing system of bookkeeping medical records is lacking privacy as well as interoperability. Currently, blockchain can offer an infrastructure for the integration of medical records among different healthcare facilities as well as data integrity features through its immutable ledger technology. Blockchain is capable of establishing a robust and secure transparent framework of storing digital medical records that brings quality services for the patients as well as reducing treatment cost. B Shen et al., have proposed a permissioned blockchain based framework named MedChain, which is built upon Hyperledger Fabric that provides the patients full control over their own medical records. The patients have the ability to share access to their health information to doctors or health centers using this distributed storage platform. Deloitte also published a paper (2016) on the opportunities for health care through blockchain based solutions. This

paper describes how interoperability in the healthcare system can be achieved by using smart contracts as well as by eliminating intermediaries to reduce additional costs and make the system more robust.

1.2 Technical Background

Bitcoin, a cryptocurrency and payment system first introduced in 2008, is one of the most well-known implementations of blockchain. The transfer of digital assets, such as bitcoin, within a blockchain is initiated when a seller or payer submits a transaction (Figure 2). These transactions are broadcasted to every peer connected to the blockchain network where clients, called miners, use a cryptographic algorithm to validate the transaction. This validation solves 2 key problems that previously existed with digital currency exchange: ensuring that the digital asset exists and that it has not already been spent. A transaction is said to be valid if a miner deems it is well formed (the input and output contain only the fields that are defined in the protocol), and the outputs it attempts to transfer exist. Miners are not certified and can be anyone who volunteers to invest their resources. The incentive for miners comes in the form of the bitcoin, which is generated and rewarded to the miners for every block of transactions validated. The software required to mine is free to download and simple to run.

TOOLS USED

1. **Smart contract(s)-** A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. The funds can be held in a Smart Contract there are rules according to which funds can be spent are specified and the smart contract is self-enforcing.
2. **Ganache-** Ganache is used to set up a personal or local Blockchain for Ethereum distributed application development. It comes with both UI and CLI interface, UI is a desktop application supporting the Ethereum technology. CLI interface is a command line interface which will be used for making a decentralized blockchain

network for the application.

3. **Truffle-** Truffle is the development environment, testing framework, and the dApp pipeline for an EVM blockchain. This description might sound somewhat abstract for most people, so we will break down what this means. However, this breakdown is just on a fundamental level, and there is much more to learn about Truffle.

Software Requirements

- Operating System- Linux (For development)
- Web browser- Chrome (latest) or Mozilla Firefox(Latest)

HARDWARE CONFIGURATION

- COMPUTER: Personal
- Processor: Core 2 Duo or more
- RAM: 2 GB or more.
- Hard Disk Drive: 320 GB or more
- .Monitor: 15 inch color Samsung or more.
- Mouse: Logitech
- Keyboard: Board with 104 Keys or more

Once a transaction is validated by a configurable number of clients, it is stored in a block, which contains the details of validated transactions, along with a timestamp and a cryptographic hash (a mathematically generated alphanumeric string) of the data. The block with the transaction information is added to the end of the blockchain, which is followed by the transfer of assets to the receiving party. The one-way, cryptographic hash is an important aspect of the blockchain because this value forms a distinct, digital signature that is unique to the current block of data and is created using the hash of the block preceding it (Figure 5).

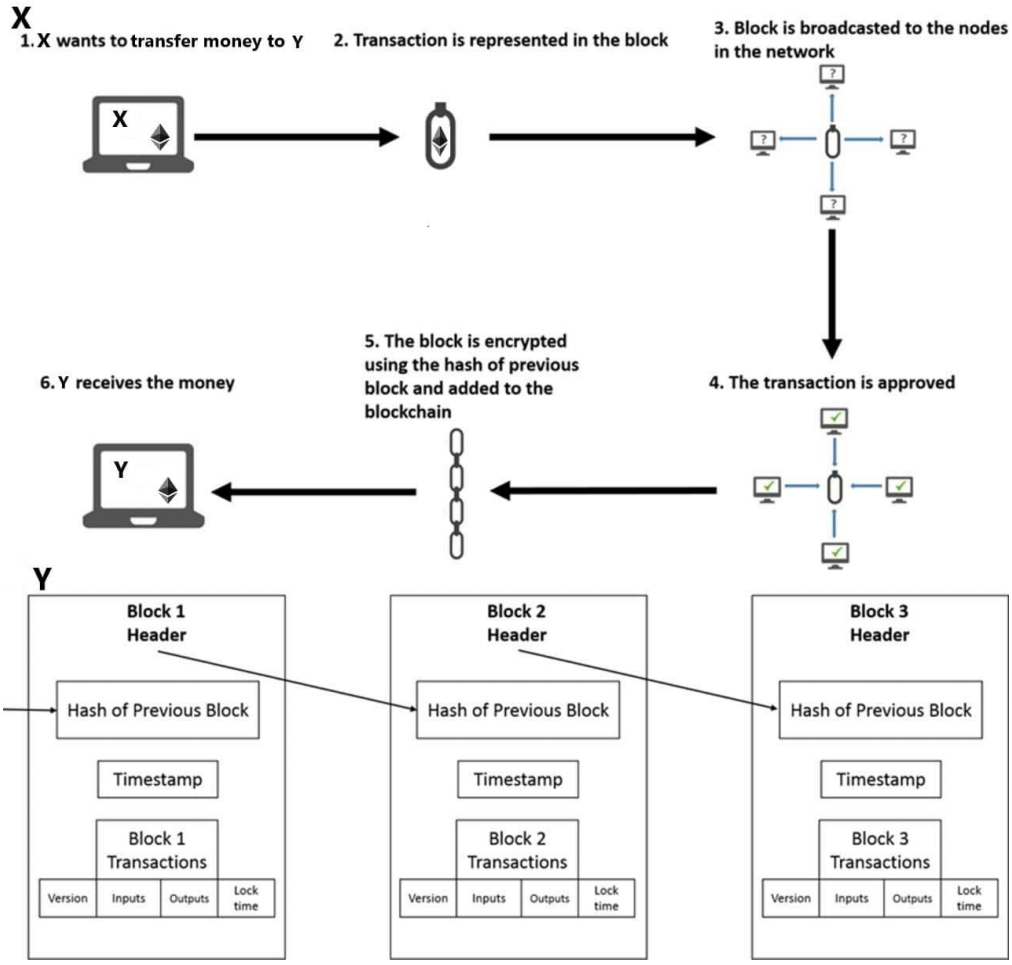

FIGURE 5: Functionalities of the System

CHAPTER-2 Literature Survey

2.1 Literature Survey

A lot of writing was inspected on blockchain based activities identified with the clinical business wherein a portion of the work centers basically around the information stockpiling perspective. As per the writing audit about existing programming stages, functionalities, systems, and innovations that have been utilized previously, the accompanying significant contemplations have been recognized and summed up in Figure 6.

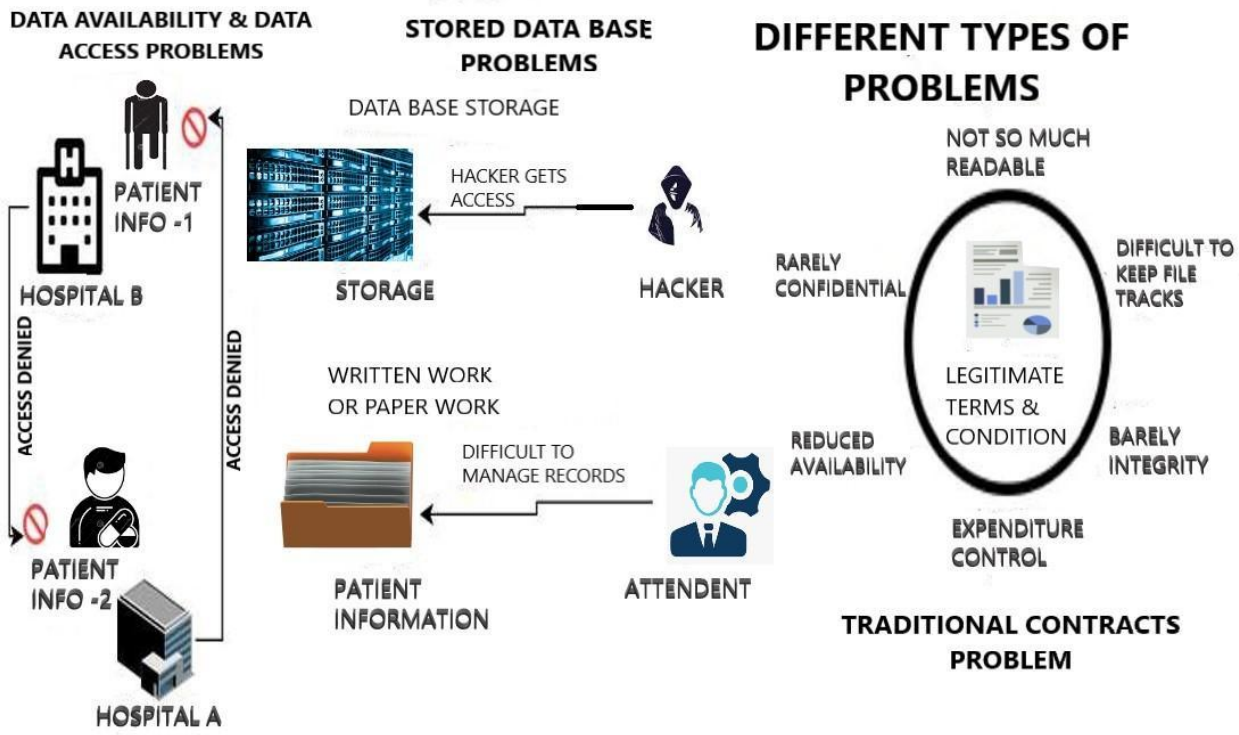

FIGURE 6 : Different problem in HRE

As displayed in Figure 6 considering the information access and accessibility, interoperability is recognized as a central point of contention in current information stockpiling and sharing frameworks. This issue concerns the shortfall of a predictable and viable philosophy for sending, getting, and taking care of information between medical services substances.

The use of blockchain innovation in medical care has turned into a recent fad in the data innovation space.The accompanying segment sums up key discoveries in regards to the abovementioned.

Specialized and business difficulties and advantages for the reception of blockchain in the medical care industry, has been plainly referenced in Applications of Blockchain in Healthcare: Current Landscape and Challenges, which was distributed by. Katuwal, G. et al in 2019.

Blockchain application with wellbeing token in clinical and wellbeing modern, that was distributed by Chi Kin, Lee in 2018 has included more subtleties model use instances of blockchain in the wellbeing business and the possible advantages of utilizing such a technology.

Harshini V. M. et al of a school of gadgets and media transmission designing at REVE University, introduced an exploration paper about Bangalore India introduced wellbeing record the executives through blockchain innovation research paper.
Data from reasonably-priced cellular gadgets and wearable sensors is developing at an exponential charge. Distributed architectures based totally on commodity hardware offers value efficient excessive scalability.
Ariel Ekblaw et al at MIT Media Lab, Beth Israel Deaconess Medical Center introduced a white paper in August 2016 about the blockchain in medical services called MEDREC and It is a decentralized record of the executives framework to manage HERs(Health Care Electronic Record).

2.2 CHALLENGES

Following, we identified some of the potential challenges for building blockchain based healthcare systems that need to be addressed properly before the actual deployment.

A. Scalability Restrictions:

One of the potential challenges in blockchain healthcare would be scalability. The trade-off between the available computing capabilities versus the amount of medical transactions could limit the scalability of such healthcare systems .

B. High Development Cost:

The blockchain based healthcare systems may take high development and operation costs. The government and healthcare sector still need to define the different kinds of

development, operations and total deployment cost for all involved stakeholders. Thus, it is crucial to find the optimal ways to reduce the overall cost and resources for building such systems.

C. Standardization Challenges:

For the successful deployment in healthcare applications, appropriate standards must be defined by standardization bodies. For example, in the case of healthcare information stored on the blockchain, it should be made clear what data, size and format can be sent to the blockchain. Thus, it must be defined well what medical data is stored on or off the blockchain.

D. Cultural Resistance:

The current society is mostly habitual of such healthcare processes that are accessed either through paperwork based procedures or in some cases through online means such as EHR/EMR and other online health services. In the current time, the patient's data is not so commonly shared with multiple parties. Therefore this cultural shift will be one of the major challenges as changing the behavior of the people towards data sharing in a distributed way will require some effort.

E. Regulatory Uncertainty:

Regulatory bodies would face challenges in order to define the policies that will consider the collaboration of various stakeholders to draft a complete ecosystem that also takes into account the existing regulatory framework. The Health Insurance Portability and Accountability Act (HIPAA) is also currently working on defining the standards to preserve the privacy of users' medical records.

F. Security and Privacy Concerns:

Blockchain technology with healthcare data provides some security features. However, security and privacy are still the foremost concerns in blockchain based healthcare and require concrete security solutions. For example, an authorized entity should be able to access the data and data storage and sharing must be done in a secure way.

G. Unwillingness to Share:

Some of the stakeholders providing healthcare services still hesitate to share the data with other parties. For example, hospitals and insurance payers do not want to share the data very easily to other entities. One of the reasons for this can be that the hospital may want to keep the cost data to themselves and may set different costs for different patients. Hence, the trust must be developed between various entities so that each entity should agree to share the data for better healthcare systems.

Despite the attractiveness of blockchain-associated properties and potential benefits in blockchain based healthcare applications, it is important to note that the technology is not without limitations. Challenges exist that militate against the successful use of blockchain technology in health care. Some of these challenges are discussed here, with suggested potential solutions to overcome them.

2.3 PROBLEM FORMULATION

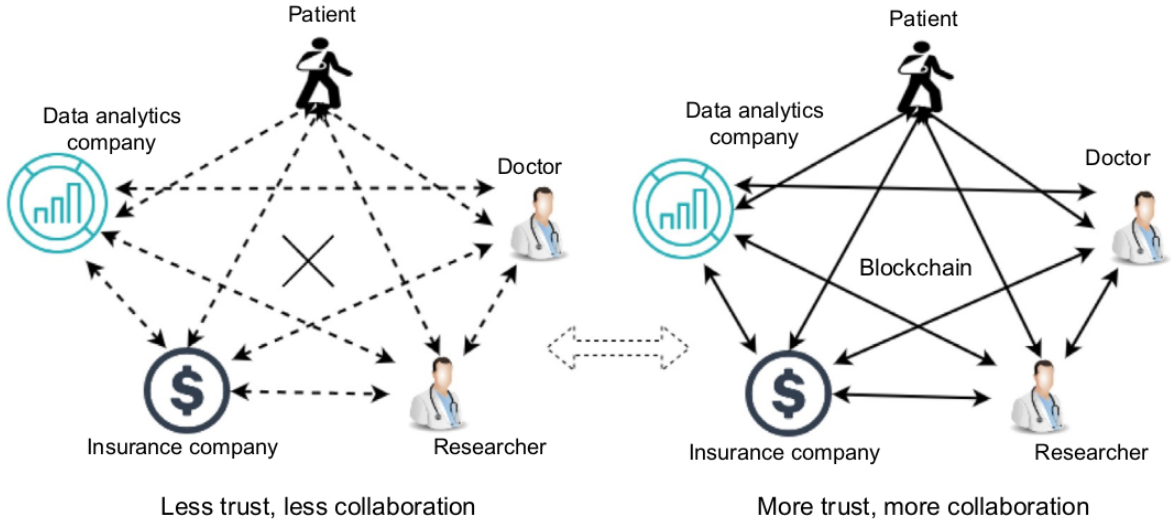

FIGURE 7: Possible changes that blockchain related to the privacy of health-care big data.

Some of the notable opportunities that would be able to revolutionize the healthcare industry with the integration of the blockchain are as follows:

Decentralized storage: blockchain stores the information, which is transparent and delivered to third parties based on the consent of the creator. A decentralized way of storing the information is keeping multiple copies of that information in multiple places. Consent: access, storage, and distribution will be controlled by the global consensus algorithm. After an autonomous sanction from all available parties, the changes are allowed to be made on the data.

Immutability: alteration of any data is impossible. Once data is stored in a particular block, it can never be changed or modified.

Increased capacity: With no middleman and less approvals complexity, blockchain is a cost- effective way of maintaining the privacy of data.

A big concern in the healthcare big data sector is the increasing amount of data as well as it's related analysis, privacy, and security. With the increasing demand for healthcare data mining, a need for a higher computing power is also increasing, which was discussed by Pattnaik et al. For the security of personally identifiable information (PII) and her, blockchain technology has already been welcomed by many researchers. This chapter identifies the effect of blockchain on healthcare big data privacy. In addition, this chapter also lists the challenges, scope, and current status of the technologies in detail. This chapter also discusses the flaws that are associated with blockchain solutions, which can be a good reference point for future study.

The healthcare sector is a problem-driven, data- and personnel-intensive domain where the ability to access, edit and trust the data emerging from its activities are critical for the operations of the sector as a whole. If we divide the operations within the healthcare sector into triage, health problem-solving, clinical decision-making, realization and assessment of knowledge-based care (Fig. 7), achieving the desired health outcomes hinges on engaging a multidisciplinary team of health personnel that apply the most appropriate knowledge, technologies and skills when dealing with the patient. When collaborating with educational institutions, the healthcare sector must provide access to patients and provide an arena for training so that students can develop and refine the necessary skills. In return, the educational institutions provide the sector with qualified personnel. When collaborating with institutions and companies with a research and engineering agenda, health institutions must assist in providing access to professionals, informants, test persons and samples. When participating in prospective clinical trials, health institutions must assist in developing, planning, conducting and reporting the experiments. In return, the research and engineering institutions provide the healthcare sector with updated knowledge, methods and tools. Hence, the activities of health institutions are tightly interwoven with institutions engaged in educating health personnel and in biomedical research and engineering.

The activities require effective interchange of consents, patient-related data and proofs, and reimbursements processes, which effectively means exchanging data across institutional borders. At the same time, health institutions are mandated to protect the highly sensitive data that patients choose to share with them.

To both maintain the patient's privacy and exchange data with other institutions in the healthcare ecosystem, access control, provenance, data integrity and interoperability are crucial. The traditional way of achieving access control commonly assumes trust between the owner of the data and the entities storing them. These entities are often servers fully entrusted for defining and enforcing access control policies

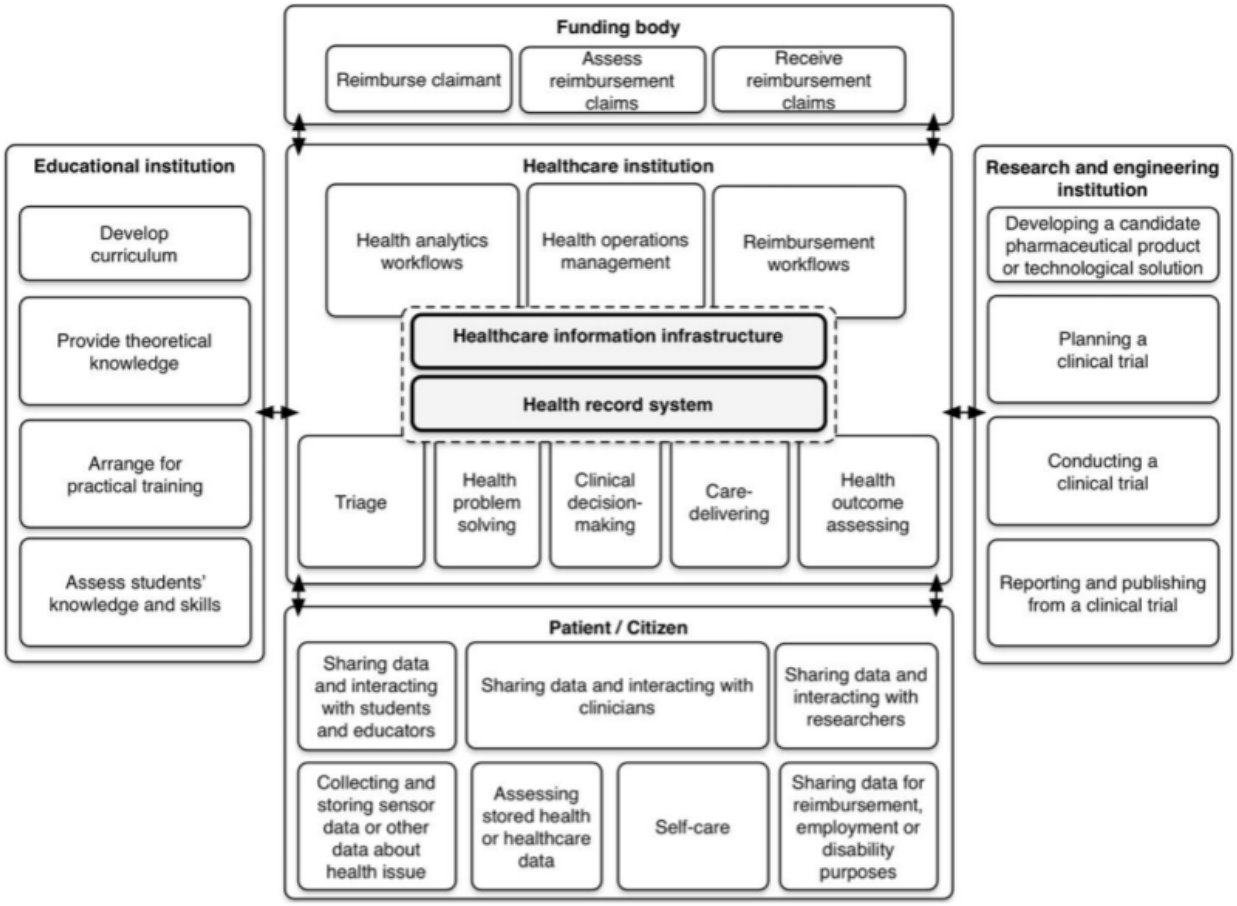

FIGURE 8: map of the health sector

Interoperability is the ability of different information systems, devices or applications to connect, in a coordinated manner, within and across organizational boundaries to access, exchange and cooperatively use data amongst stakeholders, with the goal of optimizing the health of individuals and populations. Data provenance refers to the historical record of data and their origins. In the health domain data, provenance can, for example, be to deliver auditability and transparency in EHR, and to achieve trust in EHR software

systems. Data integrity as a general definition given by Courtney and Ware is the data quality definition which deals with the expected quality of the data. This means that the degree to which the expected quality of the data is met or exceeded determines the data integrity. Healthcare institutions currently experience an increased demand of real-world data from industry and research organizations. At the same time, unauthorized sharing, and highly publicized break-ins and robbery of sensitive data constantly erode the public trust in healthcare institutions. A third problem is malpractices within the healthcare ecosystem that exploit the very same trust (e.g. the problems with counterfeit drugs, procedures, skills and patients). Taken together, this is a situation that commands rethinking and consideration of alternative approaches. With some of its key attributes such as decentralization, distribution and data integrity, and without any necessary third party, blockchain technology has many appealing properties that could be utilized to improve and obtain a higher level of interoperability, information sharing, access control, provenance and data integrity among the mentioned stakeholders, thereby moving towards a new infrastructure for building and maintaining trust.

2.4 POSSIBLE SOLUTION

1. Interoperability

The interoperability challenge stems from the fact that there is not yet a universal standard for developing blockchain-based healthcare applications; for example, applications developed by different vendors or on different platforms may not be interoperable. Consequently, there is a need to develop protocols that would ensure interoperability between blockchain networks and that would facilitate consistent storage of medical records and the seamless transfer of such records across different platforms. Current efforts are focused on developing prototypes and proofs-of-concept with less attention paid to the need for interoperability. The resulting systems are disparate blockchain-based healthcare platforms with varying levels of smart contract functionality, transaction schemes, and consensus models.

Compare and contrast, for example, HealthChain (Ahram, Sargolzaei, Sargolzaei, Daniels & Amaba, 2017) which is an EMR application developed as a permissioned, private blockchain network via the IBM Blockchain's Hyperledger Fabric (Androulaki Artem Barger Vita Bortnikov et al., 2018) v. the Ancile blockchain framework (Dagher et al., 2018), which similarly utilizes smart contracts to control EMR management, but is built on the Ethereum (Ethereum, 2015) blockchain platform. These two systems manage EMRs on very different platforms; as such, without a well defined standard, it is difficult to transfer a patient's record from one platform to the other. As data sharing is at the heart

of the design of modern EMR management systems, the whole advantage of blockchain is lost if disparate blockchain networks cannot interoperate among each other in order to exchange critically stored data.

One possible solution to the interoperability problem is to develop standard protocols that can guarantee interoperability between different blockchain products. For blockchain technology to be fully adopted and deployed in operational healthcare environments, open standards for interoperability need to be defined. Importantly, researchers should start collaborating on overcoming the interoperability issues and the standardization processes. A standards group (ISO/TC 307) currently exists to which researchers can send in their contributions (ISO, 2018). Some early research into the interoperability of blockchain has produced two broad categories of interoperability solutions, namely open protocols and multi-chain frameworks (Curran, 2018). On the one hand, the open protocols are standards that define how blockchains can interoperate and exchange data among themselves, for example, Interledger(https://interledger.org/). Multi-chain frameworks, on the other hand, are open environments that different blockchain networks can plug into and be able to exchange information, for example, Polkadot (https://polkadot.network/) and Cosmos.

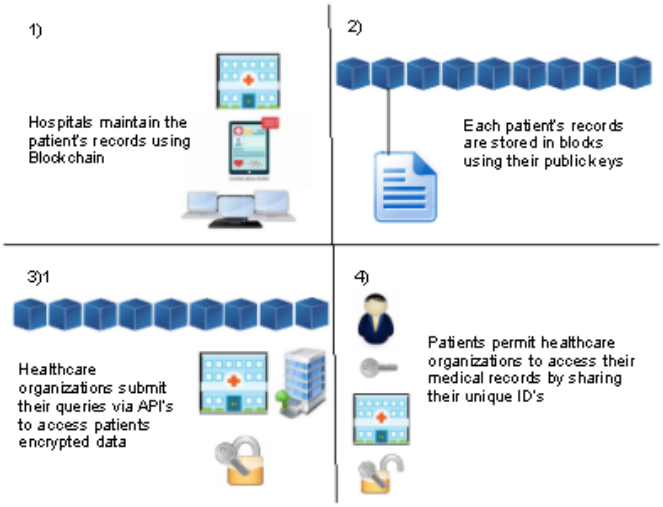

FIGURE 9: Process of managing health records

2. Security and Privacy

When it comes to security, it is evident that no one system is perfectly secure. So, even though state-of-the-art encryption techniques are employed in the blockchain, there are still potential security breaches that may be exploited to compromise the data stored on the blockchain. One famous security threat in blockchain is the 51% attack, which happens when the malicious nodes in a blockchain network outnumber the honest nodes (Kalis, Leong, Mitchell, Pupo & Truscott, 2016). Under such a circumstance, the

malicious nodes may be able to modify the data on the blockchain by undermining the distributed consensus mechanism, thereby nullifying the immutability property of blockchain.
Another security challenge is the fact that information access in the blockchain is via the private keys, which are prone to potential security breaches. On the one hand, if these private keys are stolen, it could result in unauthorized access to the stored health data; on the other hand, if the keys are lost, the stored data cannot be accessed. There is also the concern on the emergence of future technologies such as quantum computing that will be able to break the current encryption technologies upon which the blockchain is based (Engelhardt, 2017).
On privacy, the blockchain promotes transparency at the expense of confidentiality. Here, there is a concern that despite the anonymity introduced by using hashed values as public addresses, it is still possible to unveil the identity of a patient in a public blockchain by linking together sufficient data that are associated with that patient (Radanović & Likić, 2018). Moreover, there is also the potential risk of security breaches that could arise from intentional malicious attacks to the healthcare blockchain by criminal organizations or even government agencies that could compromise the privacy of the patients. Indeed, several cases of reported attacks on the blockchain-based cryptocurrencies have been reported to date (Yli-Huumo, Ko, Choi, Park & Smolander, 2016). Given the sensitive nature of healthcare data, any viable solution for managing EMRs must ensure both the integrity of the stored data and the protection of the patient's privacy.

Potential solutions to the aforementioned security and privacy-related challenges consist in following careful design and implementation techniques for blockchain-based healthcare applications to mitigate the identified challenges. For example, through the adoption of a permissioned blockchain network such as the private or consortium blockchain like ModelChain (Kuo & Ohno-Machado, 2018) instead of the public blockchain like Bitcoin, the problem of 51% attack is reasonably overcome and contained because arbitrary malicious nodes cannot hijack the network as only the authorized (honest) nodes can participate in the ModelChain network.
Similarly, another technique to mitigate the privacy issue is to store only the encrypted pointers to the real data on the blockchain, while storing actual data off-blockchain, and using the smart contracts (Swan, 2015) to automate the data management protocols as exemplified in HealthChain (Ahram et al., 2017) and Ancile (Dagher et al., 2018).
Moreover, following a rigorous software development process and applying all known security measures during code development go a long way in containing most of the security threats.
In the end, blockchain cannot fully stop all the potential attacks in healthcare cybersecurity, basically because the healthcare data would still have to be accessible and readable by the healthcare stakeholders. Accordingly, known security challenges of authentication, authorization, sniffing of credentials and data theft will continue to

persist. Nonetheless, blockchain will prove to be very effective in addressing most, if not all, integrity-based attacks because of its immutability characteristics.

TABLE 2: Law in different countries related to privacy

Country	Law	Key Factor
Angola	Information Protection Law	For sensitive information storing, processing, and collection, legal permission is needed.
United States	• HIPAA (Health Insurance Portability and Accountability Act started in 1996) • The Health Information Technology for Economic and Clinical Health (HITECH) Act, February 17, 2009	1. Right to medical record and health insurance privacy record from 12 to 18 year old citizen. 2. Meaningful use of all Electronic Health Records (EHRs).
Brazil	Law of the Constitution	Personal data and private life and citizen's image are considered as highly sensitive and secured information.
EU	Data Protection Law from Government	Protection of people's personal information during storing and processing.
Russia	Personal Data Act by Russian Federal Law	Data operators are to take all responsibility regarding any unlawful access to data.
United Kingdom	Data Protection Act (DPA)	The individual has huge power in controlling the movement of personal data. Privacy information must follow the country's territorial boundary.
India	IT Act	Any kind of breaching of personal data should compensate the victim.
South Korea	Personal Information Protection Act September 30, 2011	Right, interest, and dignity of the citizen are taken care of. No territorial scope is defined.
EU	General Data Protection Regulation (GDPR)	Personal information protection regulation, in which key factors are consent from the owner, right to forget, and the territorial boundary of data.
United States	National Institute of Standards and Technology (NIST)	Security automation, public awareness, and harmonized security rules are key factors.
New Zealand	Health Information Privacy Code	Special rules of medical institutions on collection, storage, and processing of health data.
Commonwealth	National Electronic Health Transition Authority (NEHTA)	NEHTA aims to unlock eHealth system aspects to improve the electronic health record collecting and exchanging ways.

3. Scalability and Speed

Scalability of blockchain-based healthcare solutions is a well-known challenge especially occasioned by the volume of data involved. It is not optimal, or even possible in some cases, to store the high volume biomedical data on blockchain as this is bound to cause serious performance degradation. The scalability problem is directly related to the processing speed. Depending on the protocol in use, the blockchain-based processing can introduce some significant latency, which in turn limits the scalability of the system. Similarly, the Bitcoin-based PoW protocol executes on average 288,000 transactions per day, which is very small when compared to Visa credit cards that can execute up to 150 million transactions per day (Kuo, Kim & Ohno-Machado, 2017). Hence, for real-time and scalable healthcare applications, such as continuous RPM, blockchain may prove inefficient. Possible solutions to the scalability and speed problem include the use of blockchain merely as an index for healthcare data, containing only some condensed information about the data and how they can be accessed, while the actual healthcare data is stored off-blockchain (Esposito, De Santis, Tortora, Chang & Choo, 2018; Kaur et al., 2018). However, this countermeasure removes the benefits of redundancy and continuous availability that the blockchain should ordinarily provide for the healthcare data. Further, the speed problem associated with consensus algorithms such as PoW used in some public blockchains can be mitigated by using the permissioned blockchain in which only some nodes are permitted to participate in the consensus and validation processes (Ahram et al., 2017).

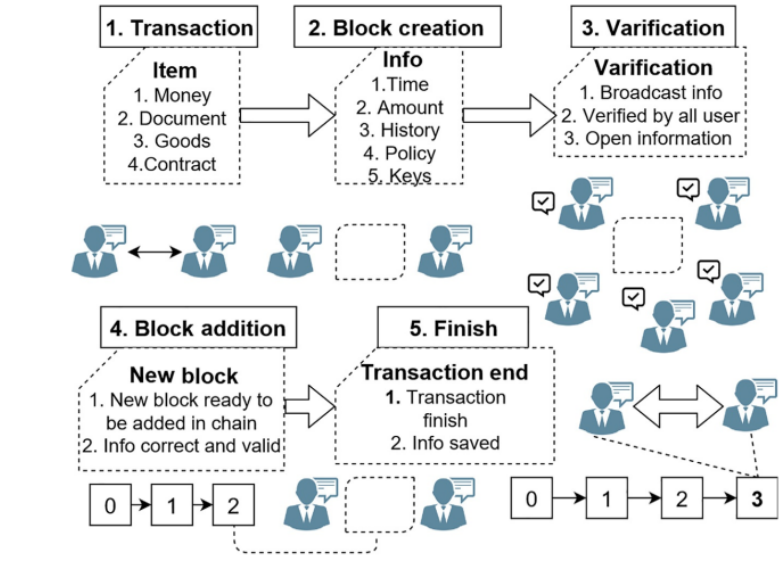

FIGURE 10: How block creation works

4. Stakeholders Engagements and Lack of Incentives

Engelhardt (2017) noted that “Blockchain technology is only as good as its users”. The technical complexity of blockchain is one of its limitations. Awesome stakeholders may find it difficult to grasp how to use the technology. Despite its many promises, if the blockchain technology is misused, the outcome will be undesirable. For instance, if some invalid or inaccurate data are stored on the blockchain, the immutability property of blockchain will only ensure that the inaccurate data are immutable, which is of no real value in this case. The vision of blockchain in healthcare isto transfer control and ownership of healthcare data to the patients; however, the patients especially the elderly and the young may be unable or unwilling to participate in the management of their health data (Radanović & Likić, 2018). This problem is echoed in Engelhardt (2017) where it is noted that if patients are unaware of what to do with their health data and how to manage them using the blockchain, they will invariably involve others to manage the data for them, which eventually nullifies the whole idea of using blockchain to empower the patients in the control of their personal health data.

A possible solution to stakeholder engagement is to engage in stakeholder education,simplifying the concept of blockchain and how it can be used to better manage healthcare resources. Also, the design and implementation of blockchain-based healthcare applications should then take into serious consideration the utility as well as usability of the system, and the integrity of the data before and after it is stored on the blockchain. Clear incentives should exist to encourage healthcare stakeholders to adopt blockchain-based solutions. There should also be ways to mask the complexity of the underlying blockchain technologies, for example, the private keys should be easy-to-use by the stakeholders but not become easily compromised.

CHAPTER-3 Functionality of the Project

3.1 Functionality

This takes a look at proposes a gadget to enhance the present day gadget shape of traditional revealed form-based file. There are several loopholes in this traditional approach inclusive of the integrity of the files. To efficiently manage authorization, this look proposes a smart agreement to register and the verification of the affected person, other scientific help industries and the medical data. Smart contracts are traces of code which are saved on a blockchain and robotically executed while predetermined phrases and conditions are met .

In this proposed system, each health center, coverage entity, research entities are involved as main nodes.

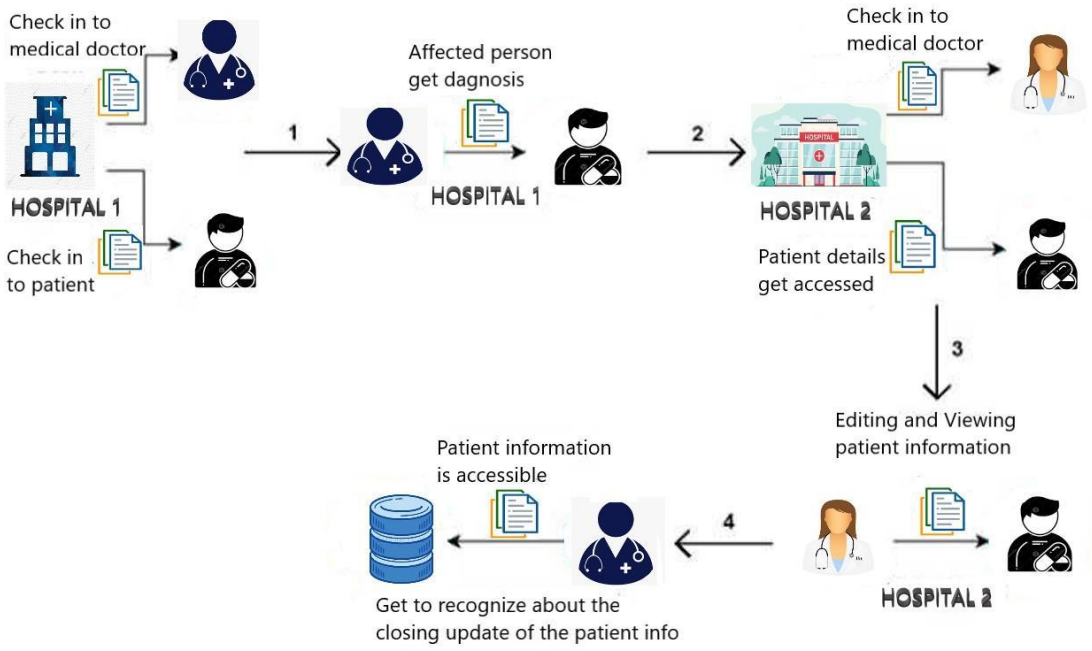

FIGURE 11: Smart contract Impact in Registration & Data Retrieval

A Smart Contract is an integral part of blockchain based applications. It is an agreement made among various involved parties in the defined system. A smart contract is a computer protocol that follows specific rules, codes and constraints agreed by all participants in the network. For example, a smart contract for banking transactions or financial purposes includes all the terms and conditions agreed by each stakeholder available in that process.

The traditional contracts are considered to be lengthy and experienced as a resource consuming process that is made either in form of writing or any actions. In contrast, smart contracts are computer based digital programs which are self-executive when the required terms are fulfilled. Healthcare systems enable a number of relevant parties to work collaboratively and efficiently for better and enhanced medical services. Therefore, defining appropriate rules in the smart contract for healthcare will be crucial and must include the consent of all the relevant parties. In the healthcare blockchain, the patient and other stakeholders in the network should set up their details and sign the agreement for accepting the terms in order to develop the requirements in the smart contract .

For example, which hospitals can store and share the patient data, which doctors can access and append the data and what kind of data is available for pharmacy and laboratory. Figure 11 highlights the use of smart contracts in blockchain based healthcare systems where multiple service providers are operating. Once the appointment between patient, healthcare providers and pharmacists specified in the contract takes place and the transaction containing information about the data arrives at the address of the smart contract, then the distributed virtual machine of the blockchain executes the programming code process. Some of the fundamental elements which smart contracts for the healthcare may contain is shown in figure 11, for example; Address specifies the address for the patient’s data on the database and address itself can be stored in blockchain; Access − code is a number that denotes to whom the patient gives permission of accessing the information such as doctor or any third party like relatives and friends; state represents the variables or function in the system and code specifies the agreement in which stakeholders signed it and other function to be performed.

Once they agree to the terms, then the transaction details will be recorded in the system and also the other entities will receive the transaction information. As compared with existing available contracts, a smart contract is faster as well as it also decreases the time for executing and deploying the patients data. Since it is a decentralized system, no one can act as a patient or healthcare provider. This system is relatively more safe to protect any medical document. Hackers cannot be able to modify or edit the document without the patient's permission.

A Smart Contract can directly deal with the stakeholders, whose signature is in the legal agreement. A Smart contract is considered as more cost-efficient because it will use less resources and eliminate the additional costs. Smart contracts are more trustworthy by having the property of immutability which means no one can modify /edit or delete the patient data without the patient's permission and this can automatically encrypt the protocol/rules. The Smart Contract simplifies the transaction happening in the Blockchain and makes it easier to perform . In addition to the useful advantages of building smart contracts, there are also needs to address some challenges for successful utilization of smart contracts in healthcare systems.

For example, if the codes or rules are written wrong (having some error) then the process will make a mistake. Without programmable knowledge, it's not easy to write or understand the algorithm and if the mistakes happen in the code, then it is very costly to fix a bug. There is also an issue with the legal framework in a smart contract as this is not validated by the government completely. A Smart Contract needs an invoking support to perform some tasks, meaning that it cannot perform automatically without any action or support .

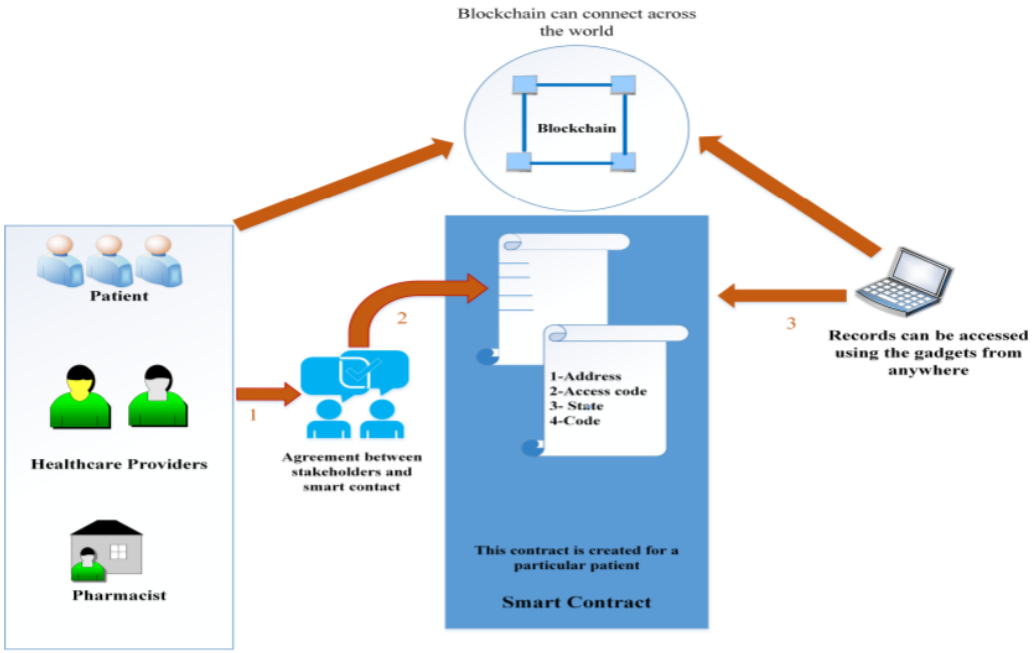

FIGURE 12: Smart contract for healthcare scenario

Smart contracts are self-executing contracts with the terms of the agreement between two parties being directly written in the form of code without the involvement of a third party. It is a protocol that digitally facilitates, enforces and verifies the negotiation or performance of the contract. In our work, the proposed concept is developed as a contract

by the name healthcare which consists of 2 nodes that is equivalent to two people and can be assumed as hospital admin / lab admin. A structure is created and named as a record which comprises patient's address, patient's unique ID, test name, date, hospital name, price, is value, signature count.

i) Invoking the transaction:

We have used a constructor which is public in nature and is automatically called when the Dapp is deployed. Transaction on the Blockchain network should be invoked only by hospital admin and he is the one who chooses labadmin and assigns him with a particular address.

ii) New Record Creation:

The existing records of the patient are stored in an ar- ray called Records and we have deployed a function called newRecord to add new data to the existing record by assigning values to the corresponding parameters.

iii) Validation:

For validating the record we have created a function called sign record in which we check whether the new record is already present in the existing record array or not by using signature count if it is '0' the hospital admin will sign the transaction and if the record already exists the signature count value will be'1' there will no signing of the transaction. When the value of the signature count turns out to be '2' record signed is emitted.

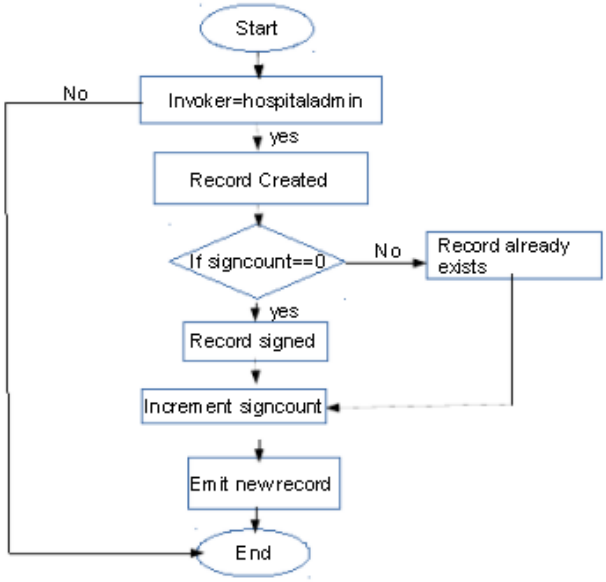

FIGURE 13: Flow chart of the smart contract

3.2 OPPORTUNITIES IN HEALTHCARE

Based on the special properties of blockchain, it can be seen that blockchain is applicable in use cases that have any of the following characteristics:
(a) two or more collaborating stakeholders exist;
(b) there are intermediaries that could be removed to improve the security and/or the efficiency of the system:
(c) trust among the collaborating entities is needed;
(d) data integrity must be maintained and
(e) there is a need for openness and transparency and/or there is a need to promote trust among the collaborating entities.

In the following subsections, several healthcare use cases representing opportunities for blockchain applications are discussed. In each case, the healthcare problem is captured and how the blockchain concepts can address the problem is illustrated. While it is not possible to cover an exhaustive list of all the potential areas of blockchain applications in health care, the review should cover those most often considered to be critically relevant.

A) Patient-Centric

EMR Management Electronic medical records(EMRs) management is concerned with the electronic creation,storage and management of patients' personal, medical and other health-related data.Capturing clinical interactions between patients and their care providers (as well as health data collected through medical sensors), provide a rich source of information, which can be harnessed to improve healthcare decisions. Yet, as Figure 4

(a) depicts, the current practice in which EMRs are stored across the different providers' databases with little or no interoperability makes it very difficult to take full advantage of these data in improving care delivery. Moreover, there is growing consensus that health data and information related to a patients' health should be readily available to the patients so that they can be active participants in their own care (Kitson et al., 2013). Other healthcare stakeholders also require different levels of access to the medical data and information; nonetheless, there is an increasing agreement that patients should be in control of what information they want to share with other stakeholders and under what conditions. Put Simply, the desired solution should be one that is patient-centric, providing the right data to the right stakeholders (patients and authorized care providers) at the right time while guaranteeing the needed security and privacy of the healthcare data being accessed.

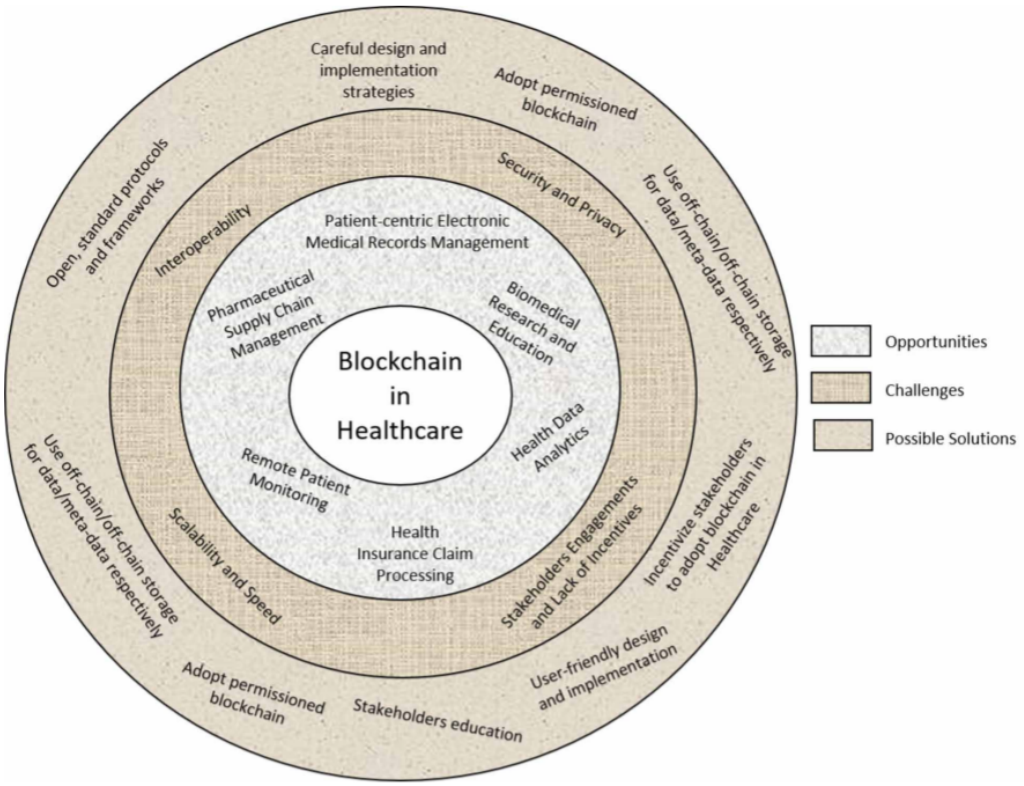

Figure 14: Summary of the opportunities, challenges, and possible solutions

Blockchain potentially offers the best opportunity to realize such a solution – a solution that can put patients at the center of managing their own health data, improve privacy and regulate access to the medical records while guaranteeing availability, and ultimately ensure data completeness by facilitating the linking and sharing of EMRs among different healthcare stakeholders, as shown in Figure 4 (b). Blockchain, with its unique properties of decentralization, immutability, auditability, reliability, and redundancy, offers many of the key features that make this technology very suitable for realizing the above objectives (Radanović & Likić, 2018).

At this point, key examples of how blockchain is being employed by the emerging blockchain startups to address the management of EMRs will be highlighted. One such example is Guardtime, a blockchain-based platform to secure over 1 million patient records in Estonia (Angraal, Krumholz & Schulz, 2017). Another example is MedRec (Azaria, Ekblaw, Vieira & Lippman, 2016), which aims at giving patients the ability to control who can access their medical record through some fine grained access permissions built onto the blockchain. The Gem Health Network (GHN) (Mettler, 2016) is yet another example, which is developed by the US company, Gem, using the Ethereum blockchain platform. GHN allows different healthcare practitioners to have

shared access to the same data. Healthbank, a Swiss digital health company, is similarly working on empowering patients to be in full control of their data using the blockchain platform (Mettler, 2016). There is also the MedicalChain project (Engelhardt, 2017), whose blockchain-based platform will facilitate the sharing of patients' medical records across international healthcare institutions, and the Healthcoin initiative (Engelhardt, 2017), which aims at constructing a global EMR system. Other recently developed blockchain-based EMR applications include the Ancile (Dagher, Mohler, Milojkovic, Marella & Marella, 2018), MedBlock (Fan, Wang, Ren, Li & Yang, 2018), BlockHIE (Jiang, Cao, Wu, Yang, Ma & He, 2018), and FHIRChain (Zhang et al., 2018).

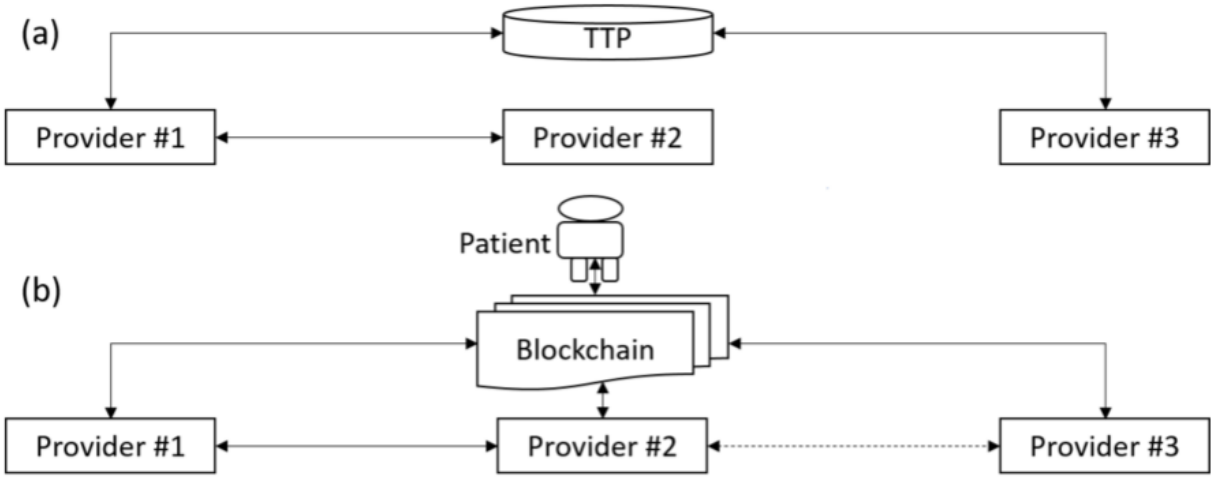

Figure 15: Comparison of existing EMR system with blockchain-based patient-centric EMR system.

4 (a) shows a case where a patient is seeing three different providers. Provider #1 and #3 can share data through a trusted third-party (TTP), e.g., Regional Health Information Organization (RHIO) with the limitations of TTP as discussed in section 2. Alternatively, two providers can exchange data if they are on the same network, i.e., have some business relationships, as in #1 and #2. Providers #2 and #3 may not be able to exchange data because they are not connected through a TTP and they are not on the same network.

4 (b) shows how this problem is resolved with blockchain which allows the patient to retrieve his data from all the three providers whenever he wants and to authorize the sharing of the data with anyone he chooses through the blockchain-enabled smart contracts. Therefore, data can be exchanged between #2 and #3 even though they do not have a business relationship, and without going through a TTP.

B) Health Data Analytics

Blockchain provides a unique opportunity to harness the power of other emerging technologies such as deep learning and transfer learning techniques to realize predictive analytics of healthcare data and advance the research in the area of precision medicine (Shae & Tsai, 2018). Boulos et al. (2018) and Roman-Belmonte et al. (2018) also noted such a use case for blockchain application in health care whereas Mamoshina et al. (2017) provides a comprehensive roadmap on how the use of blockchain in health data analytics can be realized in an intelligent fashion. Juneja and Marefat conducted experimental research in which blockchain is used in a deep-learning architecture for arrhythmia classification (Marefat & Juneja, 2018).

CHAPTER-4 Results and Discussion

4.1 RESULTS

Results from the survey were considered entirely for the implementation of the blockchain system for the scientific enterprise. A giant sample area was changed to obtained by the survey to determine the sensitivity of the facts. The sample space consisted of medical doctors, sufferers, researchers, and laboratory professionals inside the industry.

4.2 DISCUSSION

At the beginning of the research, literature evaluation found out that numerous blockchain-based total systems exist. Even though the results of those applications had been exceptional from the proposed answer, the use of the one's reviews, first authors were able to divide the main problem into four elements which are, Smart contracts, Access controls, Scalability, and Patients' live fitness tracking. Each of the proposed characteristics has unique features compared to triumphing patient info management systems. Although the patient's live health monitoring used to show up by using a wearable tool due to the impossibility of imparting the device. There is an alternative method applied to achieve the goal without harming the user requirements. The statistics which were gathered from the questionnaire, smartphone conversations, and interviewing personnel, have been useful in drafting a class model based totally on the sensitivity levels. Consequently, classified facts wish to be covered in a greenway in the course of garage, transmission, and manipulation.

The healthcare industry is facing a digital revolution because of rapid developments in Information Communication Technology (ICT). The hype regarding the utilization of blockchain in healthcare seems to be a reality in the coming future as researchers are exploring various aspects of blockchain healthcare systems. The top priority in the

healthcare landscape is to provide secure and safer means of accessing the patient's medical information throughout the whole process. Blockchain technology is assumed to be among one of the suitable ways of storing and sharing the medical information and by this only authorized entities are able to access the healthcare data. The potential of blockchain in healthcare is being realized by various involved stakeholders and its immense impact to improve the healthcare industry in terms of better medical services for the required patients and enhanced healthcare economy and revenues. One of the vital on-going obstacles in the current EHR systems is lack of nationwide healthcare interoperability and blockchain is the potential technology to handle this issue to some extent.

Apart from other questions, blockchain should address the concerns regarding the storage of medical data. As blockchain itself is very restricted in terms of storing the actual healthcare data, there is wider scope to propose concrete solutions for secure storage of the medical information. One solution for this is already available in the literature which offers to store the actual data in the server/database and the address of that data can be stored in the blockchain. The data retrieval or append and other operations can be done using that address which is stored in blockchain and linked with the database. In addition, concrete answers are also required for various security measures, for example what kind of security (symmetric/asymmetric) is more suitable for such healthcare applications and how things like key management will be handled. Moreover, certain healthcare use cases require solutions that should be anonymous, transparent and repudiation.

The future of blockchain in the healthcare sector seems to be quite prominent and visionary. However, the practicality of the healthcare application using blockchain is mostly untested yet. But with the features that blockchain promises to add in the current healthcare systems would enable improved and better quality of healthcare services. Blockchain technology will empower the patients to take more control of their medical data and can handle their healthcare information in appropriate ways for managing overall health conditions. By this, an accurate, faster and improved data sharing healthcare mechanism could be drafted that can fulfill the needs of current healthcare requirements and also facilities the patients with the desired medical services.

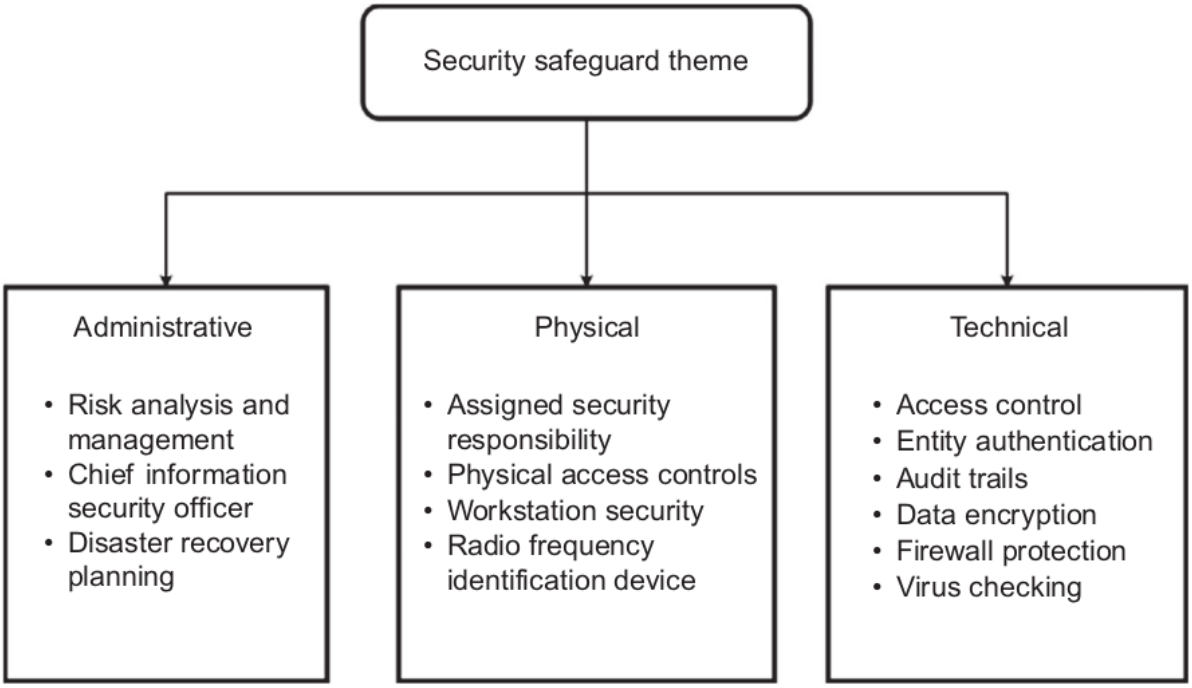

FIGURE 16: Techniques in Security safeguard theme

Three commonly used security techniques are mentioned in this study: administrative, physical, and technical safeguards. These techniques are illustrated in Figure 14.

CHAPTER-5 Conclusion and Reference

5.1 CONCLUSION

In this paper, the authors introduce a blockchain-based total platform for control of patient information that's known as Flexi Medi. Although some adjustments are essential to great track the solution for production scale, key dreams and objectives are finished. Further improvement and upgrades could make the proposed answers a green and effective platform for each the network and health care enterprise. Even though all implementation has successfully completed in step with the modern-day user expectations by using the above-stated technology and techniques, from the requirement accumulating to the consequences of the studies can be modified in keeping with the future person necessities. Researchers could be addressing the essential requirements and will do the version management thus. Additionally, blockchain answers that's included thru both the cellular utility and web software provide a consumer-pleasant street to engage with Flexi Medi offerings. It is likewise essential to word that all these functions are carried out while respecting and adhering to regulatory prerequisites which include HIPAA and GDPR making it suitable for the industry to adopt without any hesitation.

So it is more important to keep our health records safe. The world has started moving towards patient-driven interoperability where patients provide 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. This drift from an institute-driven to patient-driven comes with a bundle of challenges which are effectively addressed by Blockchain by decentralizing the whole mechanism in contrast to the traditional way of data management. 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 authenticates and authorizes the data.

Our approach also deploys smart contracts, which is a code, which executes on its own when both the parties agree on the set of protocols. Here we consider the Hospital admin as one end user and the patient as another party. There are three steps of executing the smart contract namely, Invoking, Record creation, and Validation. Our paper suggests Blockchain technology as one of the possible solutions for the efficient maintenance of health records. Blockchain technology’s use case is not restricted to health record management, it can also be implemented in various domains such as utility payments,

banking, e-voting, transport, supply chain management, etc. Further research can help implement Blockchain in all domains making lives easier.

5.2 Future Scope of Blockchain Technology

The researchers believe that Blockchain has immense potential in both academia and industry. In this section, we have briefly discussed different future scopes for the Blockchain technology including standardization, asset protection, big data, and smart contract.

Blockchain performance to lure investors by promising a huge profit. It is compulsory to know whether this technology fits the requirements before adopting it into a business solution. Hence, there should be a standard testing mechanism for blockchain-based solutions to determine its importance as well as the tradeoffs. This process could be categorized into two phases; standardization and testing phase. The first phase will verify the claims of developers regarding their blockchain solutions based on some specific criteria. The testing phase is to determine the performance of the blockchain-based solution. For instance, the owner of an online retail business cares about the performance of the blockchain-based solution. Therefore, there should be some testing and standardizing methods to test the throughput, capacity, and latency of the acquired solution platform.

Blockchain technology allows companies to create a digital trail of records of their innovations and can generate a certificate upon registering the new inventions, proof-of-concepts and designs that could prove the integrity, existence, and ownership of any IP asset. By using the unique cryptographic layer, all notarized data such as trade secrets or copyright claims could remain private and secured.

It is also believed that big data analytics could be well combined with blockchain, especially in data management and data analytics. For data management, blockchain could be utilized to store data in a secured and distributed manner. Moreover, the immutability feature of blockchain could ensure the authenticity of the data. For instance, patient health records stored in the distributed ledger would be difficult to tamper and no one can steal that information without the consent of the owner. Transactions on blockchain could be used for data analytics. In this process, it is possible to determine the potential partners' trading patterns and behaviors in the blockchain network.

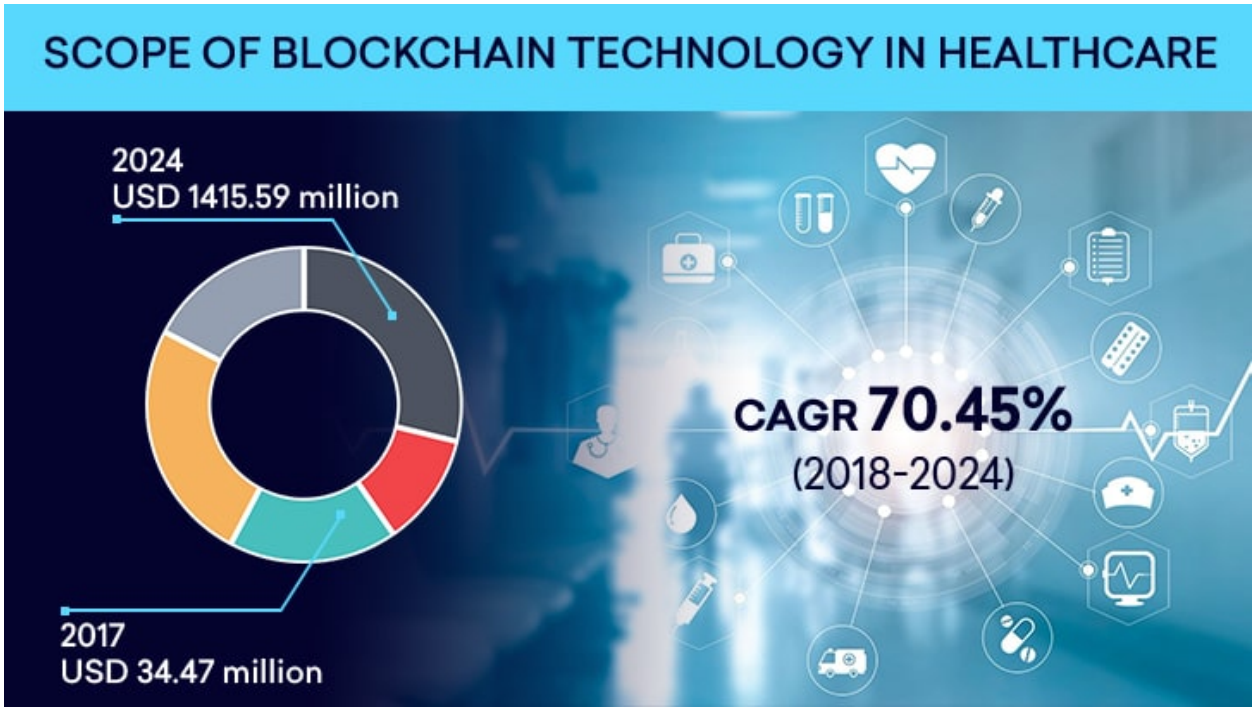

FIGURE 17: Scope of Blockchain Technology in Healthcare

Another emerging scope of blockchain is smart contract. According to Szabo et al., a smart contract refers to a digital transaction protocol that executes the rules and policy of a contract. This protocol is a piece of code that is deployed in the blockchain node. Execution of a smart contract is initiated by a message embedded in the transaction. Recently, various smart contract developing platforms are emerging. A smart contract in blockchain could be used in different application areas, such as IoT-based platforms and banking services. The research on smart contracts can be separated into two types; development and evaluation. Smart contract platform development could be performed under development. Ethereum is providing the infrastructure to deploy many smart-contract based solutions, such as car auctions, online trading, and so on. Evaluation refers to performance and code analysis. It has been proven that even a small bug in developing smart contracts could cause a disastrous impact. The precise example could be the DAO attack, where over 60 million dollars were stolen due to the recursive call bug. Therefore, it is very important to analyze the attacks on the smart contract. On the other hand, the performance of the smart contract could become an important research topic. As the blockchain technology is acquiring immense attention from public and private sectors, more smart contract-based applications would be put into use.

5.3 Some Amazing Application of blockchain in healthcare

We now know there is an immense scope of blockchain in healthcare. Here are the numerous applications of Big Pharma.

Blockchain technology helps healthcare researchers uncover genetic code by facilitating the secure transfer of patient medical records, managing the drug supply chain, and facilitating the secure transfer of patient medical records.Let's see them one by one.

1. Maintain Patient's Medical Records:

Assume you went to a doctor in 2010 for advice on a disease that was eventually treated, but the condition resurfaced in 2021, 11 years later. Now you must locate the consulting physician and hope that he has the records.

Just cut to the decentralized blockchain era, when Blockchain Technology is the norm in Healthcare. You and your current doctor will have a thorough record of what you were affected from thanks to your healthcare app that has Blockchain capability built-in. Blockchain can also be used to ensure that all medical records are accurate.

2. Supply chain management (SCM)

The present healthcare supply chain is not secure and time-consuming. The medications are first made in the production centers. They are subsequently distributed to wholesale wholesalers, retailers, and eventually to customers. To make matters worse, there's a serious threat to the pharmaceuticals' legitimacy, as substandard and counterfeit drugs can easily enter the system. Blockchain healthcare's immutability can solve multiple challenges at once.

Assuring that the active components employed in medication development meet medical requirements. Counterfeit medications can be tracked via blockchain: Healthcare and pharmaceutical companies can eliminate counterfeit pharmaceuticals by using blockchain technology. Pharmaceutical businesses,

pharmacies, and healthcare professionals all benefit from information about the flow of drugs and inventories. It's also a lot easier to manage pharmaceutical and gadget recall.

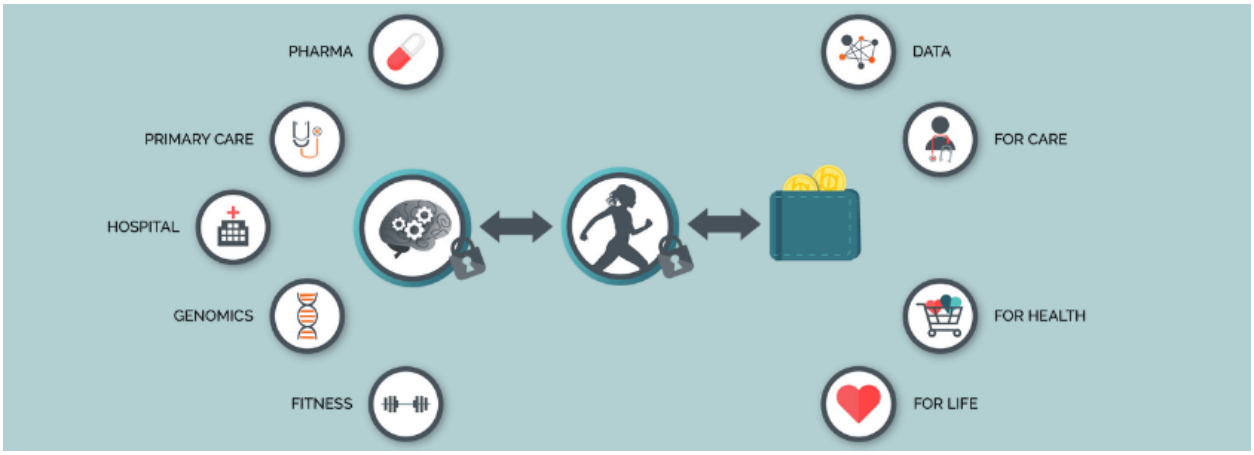

FIGURE 18: Blockchain and Healthcare: Future scope

3. Clinical Research

Blockchain has the potential to be useful in medical research. The traceability of data collected during the clinical trial procedure is critical for evaluating the suggested medical therapies. Suppose Blockchain and Healthcare are coupled in such a way that they are integrated with users' health-related IoT devices. One can get a full record of observational data and patient activities can be made. Such a study yields significant results, allowing for better drug composition that is more closely aligned with the particular needs of the consumers.

4. Treatment Regimen

Healthcare research organizations can evaluate the impact of a given treatment regimen on a big portion of a customer's population thanks to validated access to extensive patient data. This type of downstream research on the influence of a treatment regimen on a patient's well-being strengthens the foundation for continued intervention modification to fit the patient's unique characteristics.

5. Settlement Resolution

One of the things that irritate the healthcare business is the amount of time spent on claim settlements. The terms and conditions of the contract between the payer and the provider are defined using smart contracts on the blockchain.

6. Shift in the business model

When blockchain is integrated into healthcare processes, it can develop new business models. Let’s look at various examples of how blockchain affects stakeholder business models, such as Blockchain healthcare.

REFERENCE

[1] F. BOIANI, “Blockchain-Based Electronic Health Record Management For Mass Crisis Scenarios”. DEGREE PROJECT IN COMPUTER SCIENCE AND ENGINEERING, SECOND CYCLE, 30 CREDITS STOCKHOLM, SWEDEN, 2018, p. Ninety-two [Online]. Available: http://www.Diva-portal.Org/smash/get/diva2:1335811/FULLTEXT01.Pdf. [Accessed: 14- Feb- 2020]

[2] "What is Interoperability, and What are the Benefits?", Continuum, 2020. [Online]. Available: https://www.Carecloud.Com/continuum/what-is- interoperability/. [Accessed: 07- Feb- 2020]

[3] L. Ismail and H. Materwala, "(PDF) Lightweight Blockchain for Healthcare", ResearchGate, 2019. [Online]. Available: https://www.Researchgate.Net/book/336573826_Lightweight_Blockchain_for_Healthcare. [Accessed: 10- Mar- 2020].

[4] Katuwal, G., Pandey, S., Hennessey, M. And Lamichhane, B. “Applications of Blockchain in Healthcare: Current Landscape & Challenges” 2019. [Online] Research Gate. Available at: https://www.Researchgate.Internet/guide/329525760_Applications_of_Blockchain_in_Healthcare_Current_Landscape_Challenges [Accessed 17 Feb. 2020].

[5] Lee, C., “Blockchain Application with Health Token in Medical & Health Industrials”, 2020. [Online] ATLANTIS PRESS. Available at: https://dx.Doi.Org/10.2991/ssphe-18.2019.Fifty five [Accessed 17 Feb. 2020].

[6] V M, H., Danai, S., H R, U. And R Kounte, M. (2019). [Online] ResearchGate. Available at: https://www.Researchgate.Net/ebook/336439409_Health_Record_Management_through_Blockchain_Technology. [Accessed 17 Feb. 2020].

[7] A. Linn, L. And B. Koo, M.D., M. (n.D.). [online] Healthit.Gov. Available at: https://www.Healthit.Gov/sites/default/files/11-seventy four-ablockchainforhealthcare.Pdf. [Accessed 18 Feb. 2020].

[8] Ekblaw, A., Azaria, A., Halamka, J. And Lippman, A. (2016). [online] S3.Amazonaws.Com. Available at: https://s3.Amazonaws.Com/academia.Edu.Files/61480915/A_Case_Study_for_Blockchain_in_Healthcar20191210-107055- 1pdo5bw.Pdf. [Accessed 20 Feb. 2020].

[9] D. Di Francesco Maesa, P. Mori and L. Ricci, Blockchain-Based Access Control Services. Halifax: The 2018 IEEE International Conference on Blockchain, 2018 [Online]. Available: https://www.Researchgate.Net/publication/330468939_Blockchain_Based_Access_Control_Services. [Accessed: 07- Mar- 2020]
[10] Blockgeeks. 2020. “What Is Ethereum Gas?” [The Most Comprehensive Step-By-Step Guide!]. [online] Available at: https://blockgeeks.Com/publications/ethereum-gasoline Security Wiki", Secret Double Octopus, 2020. [Accessed: 06- July- 2020].
[11] Aragon.Org. 2020. Library Driven Development In Solidity. [online] Available at: https://aragon.Org/weblog/library-pushed-developmentConsensys. [Accessed 29 August 2020].
[12] Proposals, E., 2020. EIP-1167: Minimal Proxy Contract. [online] Ethereum Improvement Proposals. Available at: https://eips.Ethereum.Org/EIPS/eip-1167 [Accessed 29 August 2020].
[13] A. Roan, "Proposing Future Ethereum Access Control", medium.Com. 2020 [Online]. Available: https://medium.Com/coinmonks/offering-destiny-ethereum-access-manage-72e56e14e68e. [Accessed: 07- Jul- 2020]
[14] K. Rege, N. Goenka, and P. Bhutada, "Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA", Citeseerx.Ist.Psu.Edu, 2013. [Online]. Available: http://citeseerx.Ist.Psu.Edu/viewdoc/download?Doi=10.1.1.402.8867&rep=rep1&kind=pdf. [Accessed: 11- May- 2020].
[15] J. DE GROOT, "What is HIPAA Compliance? 2019 HIPAA Requirements", digitalguardian.Com, 2020
[16] N. Ismail, "6 steps to GDPR compliance", Information Age, 2017. [Online]. Available: https://www.Facts-age.Com/6-steps-gdpr- compliance-123466406/. [Accessed: 08- Jul- 2020].