SWASTHYA MITRA: SMART CONTRACT ENABLED PATIENT'S ELECTRONIC HEALTH RECORDS (EHR) SHARING SYSTEM

A Thesis Submitted
In Partial Fulfilment of the Requirements
for the Degree of

MASTER OF COMPUTER APPLICATIONS

By

Kajal Punia
(University Roll No. 2000290140055)

Niharika Baliyan
(University Roll No. 2000290140058)

Under the Supervision of
Dr. Arun Kumar Tripathi
Professor

Submitted to

DEPARTMENT OF COMPUTER APPLICATIONS
KIET Group of Institutions, Ghaziabad
Uttar Pradesh-201206

(MAY 2022)

CERTIFICATE

Certified that **Niharika Baliyan (Enrollment No. 200029014005743)**, **Kajal Punia (Enrollment No. 200029014005740)** have carried out the project work having "**Swasthya Mitra: Smart contract enabled patient's electronic health records (EHR) sharing system**" for Master of Computer Applications from Dr. A.P.J. Abdul Kalam Technical University (AKTU) (formerly UPTU), Technical University, Lucknow under my supervision. The project report embodies original work, and studies are carried out by the student himself / herself and the contents of the project report do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.

Date:

Niharika Baliyan (University Roll No. 2000290140058)

Kajal Punia (University Roll No. 2000290140055)

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

Date:

Dr. Arun Kumar Tripathi
Professor
Department of Computer Applications
KIET Group of Institutions, Ghaziabad

Signature of Internal Examiner **Signature of External Examiner**

Dr. Ajay Shrivastava
Head, Department of Computer Applications
KIET Group of Institutions, Ghaziabad

ABSTRACT

Due to enhancement of the information technology all over the world, we shifted from an old paper-based medical record system to a digitized one which is a cloud-based system. Although it provided the world with better financial opportunities and increased the control of patients over their records. But it also has numerous downsides like being easily hackable because of a centralized storing system, privacy issues due to third-party involvement, and increased latency issues. We can get a grip on these vulnerabilities with the help of Blockchain. Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets. It is almost impossible to tamper with the data in blockchain due to the use of hashing and different consensus algorithms which ensure data integrity and security. Hashing is a cryptography process for converting any data form into a unique text string. Furthermore, a smart contract that is implemented on the Ethereum blockchain is used to make the system more effective. Smart contracts are computer programs that self-execute when predefined conditions are fulfilled. This thesis focuses on a smart contract-enabled health record system. The proposed system completely eliminates the role of third parties which enhances the privacy of a patient and makes the health record system more patient-centric.

ACKNOWLEDGEMENTS

Success in life is never attained single handedly. My deepest gratitude goes to my thesis supervisor, **Dr. Arun Kumar Tripathi** for his guidance, help and encouragement throughout my research work. Their enlightening ideas, comments, and suggestions.

Words are not enough to express my gratitude to Dr. Ajay Kumar Shrivastava, Professor and Head, Department of Computer Applications, for his insightful comments and administrative help at various occasions.

Fortunately, I have many understanding friends, who have helped me a lot on many critical conditions.

Finally, my sincere thanks go to my family members and all those who have directly and indirectly provided me moral support and other kind of help. Without their support, completion of this work would not have been possible in time. They keep my life filled with enjoyment and happiness.

Niharika Baliyan

Kajal Punia

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Abbreviation	Full form
SC	Smart Contract
EHR	Electronic Health Records
SDG	Sustainability development goals
UN	United Nations
NGO	Non-Government Organizations

LIST OF FIGURES

List of Chapters

CHAPTER 1

INTRODUCTION

OVERVIEW

Blockchain is a popular technology that has helped in the settlement of a broad variety of issues across multiple sectors. It is an immutable, tamper-proof, transparent, and safe technology. It minimizes risk, eliminates fraud, and promotes transparency in a scalable manner for a wide range of applications, blockchain is a particularly promising and revolutionary technology. It's a distributed ledger of records that is validated by a network of computers all over the world. Instead of a single central authority, the records are controlled by a broad community, and no single person has power over the records. In Blockchain anyone on the network has access to everyone else's entries, making it difficult for a single central organization to take control of the network. When a transaction is completed, it is forwarded to the network, where computer algorithms evaluate the transaction's authenticity. The new transaction is joined to the previous transaction after it has been validated, forming a transaction chain. Blockchain is a technology that has the capacity to modify our perspectives of business processes and revolutionize our economy. A blockchain is a database that saves encrypted data blocks and then links them together to build a chronological single source of information for the data. It provides instant, shareable, and fully transparent information; stored on an immutable ledger that can only be accessed by network members with authorization. A blockchain can track payments, accounts, and so on. Because the members share a common view of the facts, you can see all the details of a transaction from start to end, offering you increased confidence as well as

more efficiency. The first blockchain prototype was created in the early 1990s by computer scientist Stuart Haber and physicist W. Scott Stornetta, who used cryptographic techniques in a chain of blocks to protect digital documents from alteration. Haber and Stornetta's work undoubtedly influenced Dave Bayer, Hal Finney, and a slew of other computer scientists and encryption enthusiasts, ultimately leading to the establishment of Bitcoin, the first decentralized e-cash system. In 2008, when Satoshi Nakamoto published a paper on bitcoin named "Bitcoin: A Peer-to-Peer Electronic Cash System," he is considered the inventor of blockchain technology. The paper's abstract focused on making direct online payments from one source to another without using a third-party service. Based on the principle of cryptography, the study described an electronic payment system. Nakamoto's article proposed a solution to the problem of double-spending, in which digital money cannot be reproduced and can only be spent once.

1.1 Consensus algorithms

Blockchain performs consensus mechanisms for security purpose, the consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Burn (PoB), and so on are used in blockchain to provide the security. Some consensus algorithms are discussed in this section.

1.1.1 Proof of Work (PoW)

To produce new blocks in the Bitcoin network, the Proof of Work consensus process requires solving a computationally difficult puzzle. The process is known as mining, and the nodes in the network that participate in mining are called miners. Working of PoW is shown in the figure 1.1.

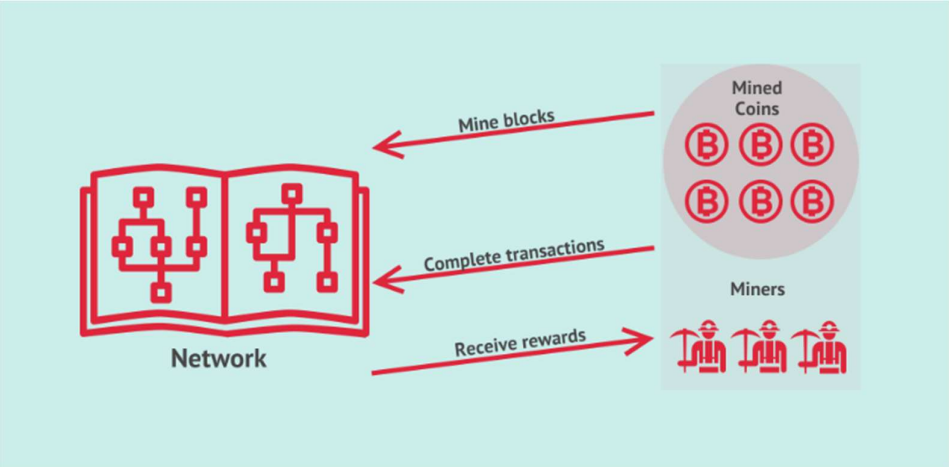

Figure 1.1: Working of proof of Work consensus algorithm

1.1.2 Proof of Stake (PoS)

Proof-of-stake is a consensus technique that blockchain utilizes to reach distributed consensus. Miners demonstrate that they have cash at stake by using energy through proof-of-work. Validators stake capital in terms of ether on Ethereum in proof-of-stake. This staked ether, therefore, serves as collateral, which may be taken away if the validator is dishonest. The validator is then in charge of ensuring that new blocks transmitted over the network are correct, as well as periodically producing and propagating new blocks. Working of PoS is shown in the figure 1.2.

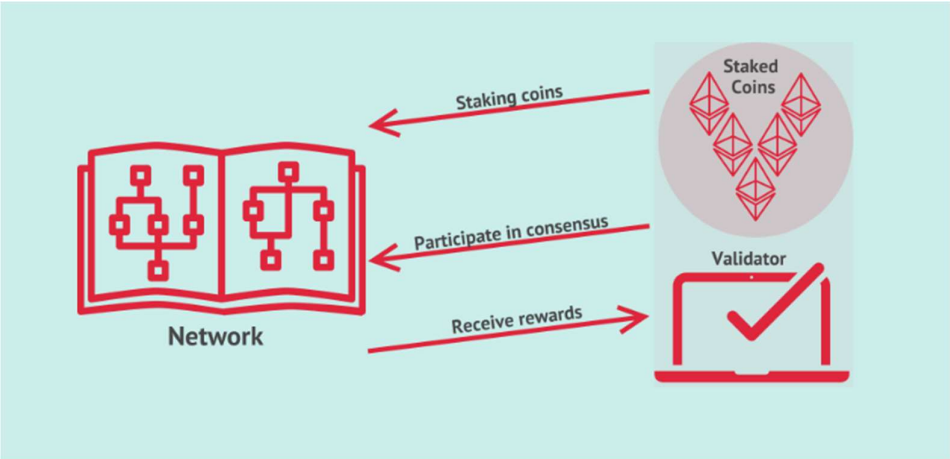

Figure 1.2: Working of Proof of Stake consensus algorithm

1.1.3 Practical Byzantine Fault Tolerance (PBFT)

Barbara Liskov and Miguel Castro proposed Practical Byzantine Fault Tolerance in the late 1990s as a consensus technique. Asynchronous systems were created with Practical Byzantine Fault Tolerance in mind. It is designed to have a reduced overhead time. Its purpose was to address a number of issues with existing Byzantine Fault Tolerance methods. Distributed computing and blockchain are two examples of application areas.

1.1.4 Proof of Burn (PoB)

Miners gain a consensus in the Proof of Burn (PoB) process by burning the currency. It's a method of permanently removing cryptocurrencies from ordinary use. The burning of coins process is used to verify transactions in such instances. As a result, the more coins a miner burns, the more likely the block will be added to the network.

In comparison with the proof of Work (PoW) system, PoB consumes less energy. In addition, unlike proof of stake (PoS) systems, PoB does not need miners to stake their coins in order to add a new block to the network.

1.2 Hashing in blockchain

Blockchain also uses the concept of "Hashing" to secure itself. Hash behaves like a fingerprint that is responsible for uniquely identifying the blocks in the blockchain. Each block contains its hash value and the hash of the prior block, the first block is known as Genesis Block. Modifying a block will change its hash value, rendering all previous blocks invalid and causing the blockchain to be rewritten. Figure 1.3 shows a hash representation in blockchain network.

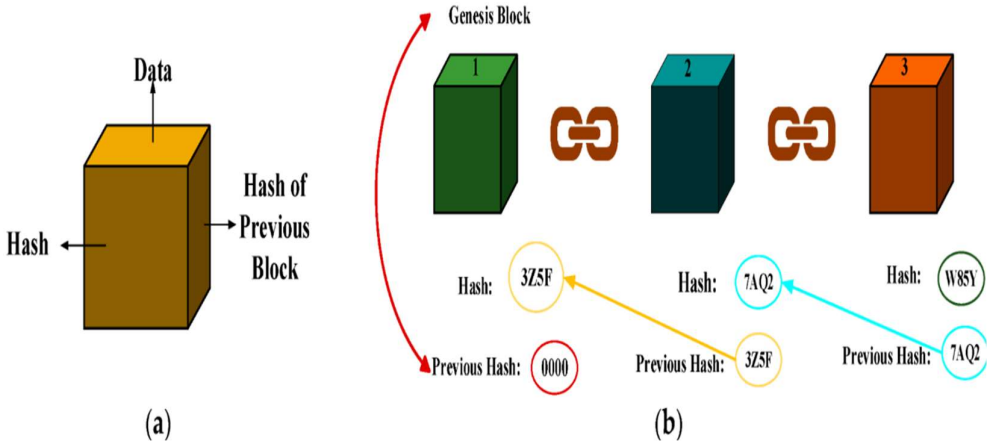

Figure 1.3: Hash of a blockchain

1.3 Types of blockchain

Blockchain is of four types, Public blockchain, Private blockchain, Consortium blockchain, and Hybrid blockchain, each of these has its own set of advantages. These are discussed in this section. Figure 1.4 shows different blockchain types in pictorial form.

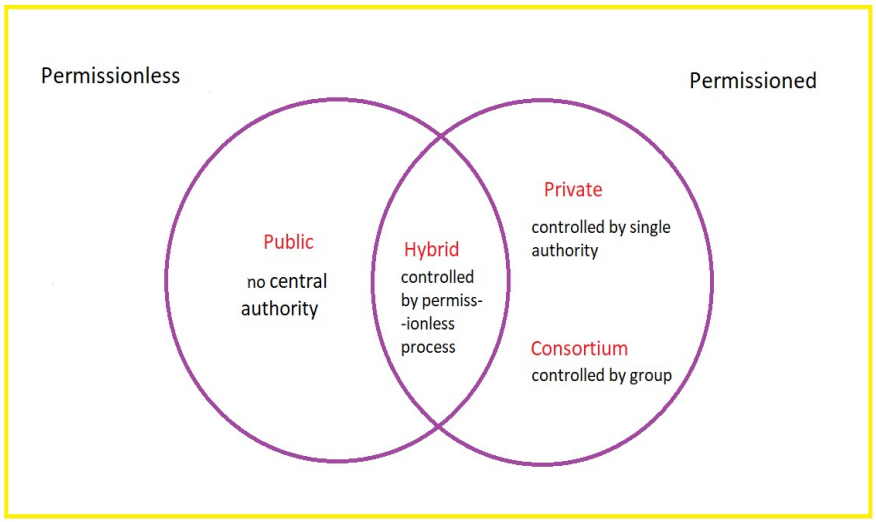

Figure 1.4: Types of Blockchain

1.3.1 Public Blockchain

A public blockchain is a permission-less distributed ledger that anybody may join and conduct transactions on. Each peer has a copy of the ledger in this non-restrictive version. This also implies that anyone with an internet connection can view the public blockchain. Permissionless blockchain i.e., public blockchain has no central authority to control it. The platform is totally open-source and it provides full transparency of the ongoing transaction. Public blockchain increases the trust between users or can say entities. But this type of blockchain gives Low-performance scalability.

1.3.2 Private blockchain

One of the several forms of blockchain technology is a private blockchain. A private blockchain is a blockchain that operates in a restricted context, such as a closed network. It's likewise a permissioned blockchain controlled by a single corporation. Private blockchains are ideal for usage within a privately held corporation or organization for internal purposes.

1.3.3 Consortium blockchain

A consortium blockchain (also known as Federated blockchains) is a novel solution to meeting the demands of companies that want both public and private blockchain functionalities. Some features of the organization are made public in a consortium blockchain, while others are kept secret. The fundamental goal of a consortium blockchain network is to increase cooperative effects in order to tackle the industry's ongoing difficulties. Consortium blockchain may be used by organizations with shared aims to improve accountability and transparency.

1.3.4 Hybrid blockchain

One of the several forms of blockchain technology is hybrid blockchain. Furthermore, the last sort of blockchain that we will examine is the hybrid

blockchain. A hybrid blockchain, in particular, may seem like a consortium blockchain, but it is not. There may be some commonalities between them, though. A hybrid blockchain combines the benefits of both private and public blockchains. It has applications in organizations that don't want to implement either a private or public blockchain and instead want the best of both worlds.

1.4 Working of blockchain

Figure 1.5 shows the working of blockchain in the simplest way possible. It shows the entire process of a transaction being completed.

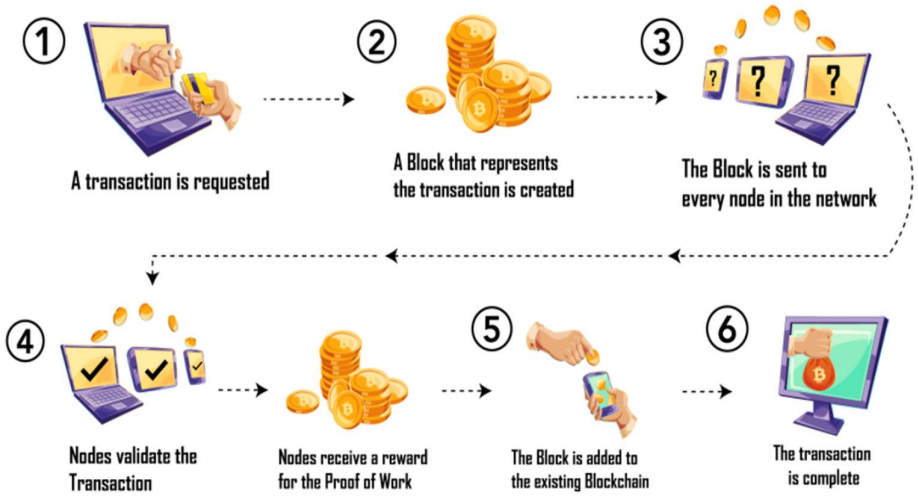

Figure 1.5: Working of Blockchain

1.5 Blockchain in healthcare

Blockchain is used in a variety of fields, including supply chain management, forecasting, healthcare, cyber-security, and finance. In healthcare systems, blockchain technology ensures safe access to patient records. The security of a patient's data is a key problem. The growing number of ransom assaults in the healthcare industry is another motive to design a safe system. Blockchain technology provides a safe platform for storing patient medical information in the form of electronic health records (EHR) without involving third parties.

1.6 Scope of Research

The main focus of this research is to provide a fast and secure electronic health record (EHR) sharing system to the patients, doctors, and laboratories for minimizing the risk, eliminating the fraud, and promoting transparency of patient health records. In the proposed system we used smart contracts which are deployed on the Ethereum blockchain to create a secure EHR system.

1.7 Research Methodology

a. Referencing research papers on Blockchain, smart contracts, and consulting with a blockchain developer.
b. The current cloud-based system has several drawbacks like security breaches, privacy issues, and high controlling costs.
c. The idea is to use multiple smart contracts for the sharing of electronic health records to overcome the issues like security and dependency on third parties.

1.8 Thesis Outline

Outline of the thesis is described below.

Chapter 1: It describes blockchain technology, its advantages, the working of blockchain technology, how blockchain secures itself with the help of consensus algorithms, and how it is used in the healthcare field.
Chapter 2: It is all about the literature review. There is the literature review from 35 papers.
Chapter 3: Introduction to smart contracts and how they are used in blockchain.
Chapter 4: It presents the deployment of smart Contracts in EHR using the Ethereum blockchain.
Chapter 5: Talks about the sustainable environment goals i.e., how the proposed system will serve society.
Chapter 6: Conclusion of the thesis is mentioned in this chapter.

Chapter 7: Talks about the possible future work regarding the proposed system.

Chapter 8: It contains the references used in the literature review.

CHAPTER 2

LITERATURE REVIEW

Literature review plays an important role for investigation of existing work. During the investigation various research papers from journals and conferences are reviewed. Some of them are discussed as follows:

- Maher Alharby, et al. [1], discussed smart contracts in blockchain. A smart contract is an executable code that runs on top of the blockchain to facilitate, execute and enforce an agreement between untrusted parties without the involvement of a trusted third party. The authors conducted a systematic mapping study to collect all research that is relevant to smart contracts from a technical perspective. The aim of doing so is to identify current research topics and open challenges for future studies in smart contract research. They extract 24 papers from different scientific databases. The results show that about two-thirds of the papers focus on identifying and tackling smart contract issues. Four key issues are identified, namely, codifying, security, privacy, and performance issues. The rest of the paper focuses on smart contracts' applications or other smart contract-related topics. Research gaps that need to be addressed in future studies are also provided in the paper.

- Zheng, et al. [2] presented an overview of blockchain architecture firstly and compare some typical consensus algorithms used in different blockchains. Blockchain, the foundation of Bitcoin, has received extensive attention recently. The blockchain serves as an immutable ledger that allows transactions to take place in a decentralized manner. Blockchain-based

applications are springing up, covering numerous fields including financial services, reputation systems and Internet of Things, and so on. However, there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome. Furthermore, technical challenges and recent advances are briefly listed. The authors also lay out possible future trends for blockchain.

- Simanta Shekhar [3] provided background on Blockchain technology, history, its architecture, how it works, advantages and disadvantages, and its application in different industries. Blockchain is one of the most important technological inventions in recent years. Blockchain is a transparent money exchange system that has transformed the way a business is conducted. Companies and tech giants have started investing significantly in the blockchain market. It has become popular because of its irrefutable security and the ability to provide a complete solution to digital identity issues. It is a digital ledger in a peer-to-peer network.

- Zibin Zheng, et al. [4] gave the blockchain taxonomy, introduced typical blockchain consensus algorithms, reviewed blockchain applications, and discussed technical challenges as well as recent advances in tackling the challenges. Blockchain has numerous benefits such as decentralization, persistency, anonymity, and audibility. There is a wide spectrum of blockchain applications ranging from cryptocurrency, financial services, risk management, internet of things to public and social services. Although a number of studies focus on using blockchain technology in various application aspects, there is no comprehensive survey on blockchain technology from both technological and application perspectives. To fill this gap, the authors conducted a comprehensive survey on blockchain technology. Moreover, this paper also points out the future directions in blockchain technology.

- N. Chaudhry, et al. [5] investigated new ways to design and evaluate different consensus algorithms. Blockchain is a distributed ledger that gained prevalent attention in many areas. Many industries have started to implement blockchain solutions for their application and services. It is important to know the key components, functional characteristics, and

architecture of blockchain to understand its impact and applicability to various applications. The most well-known use case of blockchain is bitcoin: a cryptocurrency. Being a distributed ledger, a consensus mechanism is needed among peer nodes of a blockchain network to ensure its proper working. Many consensus algorithms have been proposed in literature each having its own performance and security characteristics. One consensus algorithm cannot serve the requirements of every application. It is vital to technically compare the available consensus algorithms to highlight their strengths, weaknesses, and use cases. We have identified and discussed parameters related to the performance and security of consensus in the blockchain. The consensus algorithms are analyzed and compared with respect to these parameters. A research gap regarding designing an efficient consensus algorithm and evaluating existing algorithms is presented. This paper will act as a guide for developers and researchers to evaluate and design a consensus algorithm.

- Seh AH, et al. [6], provided detailed information about the digitization of the healthcare industry. The Internet of Medical Things, Smart Devices, Information Systems, and Cloud Services have led to a digital transformation of the healthcare industry. Digital healthcare services have paved the way for easier and more accessible treatment, thus making our lives far more comfortable. However, the present-day healthcare industry has also become the main victim of external as well as internal attacks. Data breaches are not just a concern and complication for security experts; they also affect clients, stakeholders, organizations, and businesses. Though the data breaches are of different types, their impact is almost always the same. This study provides insights into the various categories of data breaches faced by different organizations. The main objective is to do an in-depth analysis of healthcare data breaches and draw inferences from them, thereby using the findings to improve healthcare data confidentiality. The study found that hacking/IT incidents are the most prevalent forms of attack behind healthcare data breaches, followed by unauthorized internal disclosures. The frequency of healthcare data breaches, the magnitude of exposed records, and financial losses due to breached records are increasing rapidly. 5 Data from the healthcare industry is regarded as being highly valuable. This has become a major lure for the misappropriation and pilferage of healthcare data. Addressing this anomaly, the

present study employs the simple moving average method and the simple exponential smoothing method of time series analysis to examine the trend of healthcare data breaches and their cost. Of the two methods, the simple moving average method provided more reliable forecasting results.

- Vinodhini, et al. [7] investigated the privacy issues in blockchain-based electronic health systems. Blockchain-based electronic health system growth is hindered by privacy, confidentiality, and security. By protecting against them, this research aims to develop cybersecurity measurement approaches to ensure the security and privacy of patient information using blockchain technology in healthcare. Blockchains need huge resources to store big data. This paper presents an innovative solution, namely patient-centric healthcare data management (PCHDM). It comprises the following: (i) in an on-chain health record database, hashes of health records are stored as health record chains in Hyperledger fabric, and (ii) off-chain solutions that encrypt actual health data and store it securely over the interplanetary file system (IPFS) which is the decentralized cloud storage system that ensures scalability, confidentiality, and resolves the problem of blockchain data storage. A security smart contract hosted through container technology with Byzantine Fault Tolerance consensus ensures patient privacy by verifying patient preferences before sharing health records. The Distributed Ledger technology performance is tested under hyper ledger caliper benchmarks in terms of transaction latency, resource utilization, and transaction per second. The model provides stakeholders with increased confidence in collaborating and sharing their health records.

- Bahar Houtan, et al. [8] surveyed Blockchain-Based Self- Sovereign Patient Identity in Healthcare. Convergence of physical and digital identity and integration of various individual records, such as patient data, into a united repository remains a serious challenge. On one hand, collecting relevant data can help clinicians, specialists and healthcare service providers to facilitate care for patients. On the other hand, Self-Sovereign identity and the right to control personal data comes into question, because patients do not handle their data explicitly. Distributed Ledger Technology (DLT) is a novel method which would allow to securely record time-stamped data and enable patient-

driven health and identity records. In this paper, the authors reviewed the state-of-the-art in Blockchain (BC)-based self-sovereignty and patient data records in healthcare. Their motivation was to investigate the potential of BC technology for use in the patient data and identity management. As a distributed decentralized technology, BC can be very beneficial, giving patients control over their own data and self-sovereign identity. More specifically, the focus is on solutions that aim the realization of holistic BC-based Electronic Health Records (EHR) and Patient Health Records (PHR). EHR and PHR are used to record patient data, such as the doctor's notes upon a visit and radiology images. Hence, they include critical information regarding patient's privacy and identity. Therefore, development of pure decentralized Healthcare Information Systems (HIS) is a great challenge in terms of architectural and technical structure of the systems. Designing robust and reliable EHR and PHR, which represent the foundation of many other healthcare services, relies on carefully finding the balance in a trade-off between many factors, such as level of decentralization, privacy, scalability and data throughput. In this paper, the authors reviewed the state-of-the-art and provide an analysis on the design trade-offs.

- Griggs, et al. [9] presented their research on the Internet of Things (IoT) devices and other remote patient monitoring systems increase in popularity, security concerns about the transfer and logging of data transactions arise. In order to handle the protected health information (PHI) generated by these devices, they proposed utilizing blockchain-based smart contracts to facilitate secure analysis and management of medical sensors. Using a private blockchain based on the Ethereum protocol, they created a system where the sensors communicate with a smart device that calls smart contracts and writes records of all events on the blockchain. This smart contract system would support real-time patient monitoring and medical interventions by sending notifications to patients and medical professionals, while also maintaining a secure record of who has initiated these activities. This would resolve many security vulnerabilities associated with remote patient monitoring and automate the delivery of notifications to all involved parties in a HIPAA compliant manner.

- X. Zhu, et al. [10] investigated the identity management systems for the Internet of Things. The Internet of Things aims at connecting everything, ranging from individuals, organizations, and companies to things in the physical and virtual world. The digital identity has always been considered as the keystone for all online services and the foundation for building security mechanisms such as authentication and authorization. However, the current literature still lacks a comprehensive study on the digital identity management for the Internet of Things (IoT). In this paper, the authors firstly identify the requirements of building identity management systems for IoT, which comprises scalability, interoperability, mobility, security and privacy. Then, they traced the identity problem back to the origin in philosophy, analyze the Internet digital identity management solutions in the context of IoT and investigate recent surging blockchain sovereign identity solutions. Finally, they pointed out the promising future research trends in building IoT identity management systems and elaborate challenges of building a complete identity management system for the IoT, including access control, privacy preserving, trust and performance respectively.

- Arun Kumar Tripathi, et al. [11] performed a deep investigation on Blockchain Network based on Platforms and Consensus Algorithms. Due to technological growth a large volume of data is generated by various industry segments such as health care, banking system, supply chain management, agriculture, education, etc. Collected data is used for research, observation of trends and prediction of future. Security and privacy of that valuable data is the most vital aspect. To deal with data breaches and privacy issues most of industries are adopting distributed decentralized systems. Blockchain is one of the emerging technologies that helps to build analogous system in which there is no need for an intermediary or central party. This paper presents a comprehensive and comparative assessment of the blockchain. It explores and compares various type of available Blockchain network. Subsequently, various available Platform to develop the distributed and decentralized protocols are discussed, which are used to provide secure and transparent Internet services. At last, a comparative analysis among available consensus mechanisms is performed.

- M. Quinn, et al. [12] researched the different challenges in the current electronic health records, communication, and data sharing systems and presented some solutions for the same. Diagnosis requires that clinicians communicate and share patient information in an efficient manner. Advances in electronic health records (EHR) and health information technologies have created both challenges and opportunities for such communication. The authors conducted a multi-method, focused ethnographic study of physicians on general medicine inpatient units in two teaching hospitals. Physician teams were observed during and after morning rounds to understand workflow, data sharing and communication during diagnosis. To validate findings, interviews and focus groups were conducted with physicians. Field notes and interview/focus group transcripts were reviewed and themes identified using content analysis. Existing communication technologies and EHR-based data sharing processes were perceived as barriers to diagnosis. In particular, reliance on paging systems and lack of face-to-face communication among clinicians created obstacles to sustained thinking and discussion of diagnostic decision-making. Further, the EHR created data overload and data fragmentation, making integration for diagnosis difficult. To improve diagnosis, physicians recommended replacing pagers with two-way communication devices, restructuring the EHR to facilitate access to key information, and improving training on EHR systems. As advances in health information technology evolve, challenges in the way clinicians share information during the diagnostic process will rise. To improve diagnosis, changes to both the technology and the way in which we use it may be necessary.

- Arun Kumar Tripathi, et al. [13] proposed a Smart Contract enabled Online Examination System Based in Blockchain Network in their paper. In today's world, data is one of the most important assets than any other. Every user wants to secure their data from the outer world. Blockchain is the prominent technology that can provide the security and loyalty of data. Initially, blockchain has been used for the cryptocurrency and all the data were available on the public distributed ledger. But now a days, private blockchain is widely used within the organizations for data security. Blockchain engenders decentralized systems in which data can be send and receive securely and efficiently over the network. It means there is everything is hidden from the outer world; only authorized users have the

authority to read and write the data on the network. Worlds topmost industries; like the data on the network. World's topmost industries; like Walmart, IBM, Google, etc. are adopting the blockchain technology to build the Decentralized Applications (DApps). Decentralized Applications are the smart systems that are executed on a distributed computer network. Blockchain enables one of the most secure applications called Smart Contract. Smart Contracts are the computerized and secured distributed ledgers that enable secure, transparent, and tamper-proof transactions. Smart contracts create and verify the data with the help of hashing. It is a mathematical procedure that uses the most powerful algorithm cryptographic Hash Algorithm i.e., SHA-256. It engenders 256-bit signature for the input text. Ethereum Blockchain Platform is a widely used platform to build the DApps. This platform is a public network platform, which is open to all and anyone can participate in this network to send and receives the transactions. Blockchain Technology is enabled in every sector like marketing, business, education and supply-chain, etc. This paper carries out the study Ethereum Blockchain Platform in Education System. The authors have developed an application for the Online-Examination System using Blockchain Ethereum Platform with features of Smart Contracts that enables server runtime environment NodeJS and MongoDB database system. Blockchain-based system is truly more secure than all the Cloud-based systems. They have also analyzed that how blockchain based online examination is more trustworthy as compare the other systems.

- T. McGhin, et al. [14] presented the applications and research areas of blockchain in healthcare. Although big data and smart technologies allow for the development of precision medicine and predictive models in health care, there are still several challenges that need to be addressed before the full potential of these data can be realized (eg, data sharing and interoperability issues, lack of massive genomic data sets, data ownership, and security and privacy of health data). Health companies are exploring the use of blockchain, a tamperproof and distributed digital ledger, to address some of these challenges. In this viewpoint, the authors aim to obtain an overview of blockchain solutions that aim to solve challenges in health care from an industry perspective, focusing on solutions developed by health and technology companies. They conducted a literature review following the protocol defined by Levac et al to analyze the findings in a systematic manner. In addition

to traditional databases such as IEEE and PubMed, they included search and news outlets such as CoinDesk, CoinTelegraph, and Medium. Health care companies are using blockchain to improve challenges in five key areas. For electronic health records, blockchain can help to mitigate interoperability and data sharing in the industry by creating an overarching mechanism to link disparate personal records and can stimulate data sharing by connecting owners and buyers directly. For the drug (and food) supply chain, blockchain can provide an auditable log of a product's provenance and transportation (including information on the conditions in which the product was transported), increasing transparency and eliminating counterfeit products in the supply chain. For health insurance, blockchain can facilitate the claims management process and help users to calculate medical and pharmaceutical benefits. For genomics, by connecting data buyers and owners directly, blockchain can offer a secure and auditable way of sharing genomic data, increasing their availability. For consent management, as all participants in a blockchain network view an immutable version of the truth, blockchain can provide an immutable and timestamped log of consent, increasing transparency in the consent management process. Blockchain technology can improve several challenges faced by the health care industry. However, companies must evaluate how the features of blockchain can affect their systems (e.g., the append-only nature of blockchain limits the deletion of data stored in the network, and distributed systems, although more secure, are less efficient). Although these trade-offs need to be considered when viewing blockchain solutions, the technology has the potential to optimize processes, minimize inefficiencies, and increase trust in all contexts covered in this viewpoint.

- Berges, et al. [15] investigated the interoperability of electronic health records. Although the goal of achieving semantic interoperability of electronic health records (EHRs) is pursued by many researchers, it has not been accomplished yet. In this paper, the authors present a proposal that smooths out the way toward the achievement of that goal. In particular, their study focuses on medical diagnoses statements. In summary, the main contributions of their ontology-based proposal are the following: first, it includes a canonical ontology whose EHR-related terms focus on semantic aspects. As a result, their descriptions are independent of languages and technology aspects used in different

organizations to represent EHRs. Moreover, those terms are related to their corresponding codes in well-known medical terminologies. Second, it deals with modules that allow obtaining rich ontological representations of EHR information managed by proprietary models of health information systems. The features of one specific module are shown as reference. Third, it considers the necessary mapping axioms between ontological terms enhanced with so-called path mappings. This feature smooths out structural differences between heterogeneous EHR representations, allowing proper alignment of information.

- Ajay Kumar Srivastava, et al. [16] A decentralized private Blockchain implementation for academic document storage and document verification can add self-sovereignty to the process. It can dramatically minimize the time and cost of verification at various layers of verification. Blockchain would remove all the layers at all, and it will provide immediate auditing of any document. So, the request and response will be truly real time in this case. Apart from speeding up the verification process, it will also increase the security of personal education data and will check all kind of misuse also. Putting documents on Blockchain would increase the security, because all the data would only be accessible by private key and proper authentication to that private key. The authors are proposing a private Blockchain that would be managed by some private vendors and only those vendors will take part in consensus. So, they are using proof of stake consensus in this case. They are using private IPFS database server for storing our documents over Blockchain. They are considering Ethereum Blockchain ecosystem in our case.

- Ueyama J, et al. [17] surveyed blockchain based strategies for healthcare systems. Blockchain technology has been gaining visibility owing to its ability to enhance the security, reliability, and robustness of distributed systems. Several areas have benefited from research based on this technology, such as finance, remote sensing, data analysis, and healthcare. Data immutability, privacy, transparency, decentralization, and distributed ledgers are the main features that make blockchain an attractive technology. However, healthcare records that contain confidential patient data make this system very complicated because there is a risk of a privacy breach. This study aims to address research into the applications of the blockchain healthcare area. It sets out by discussing the management of

medical information, as well as the sharing of medical records, image sharing, and log management. The authors also discussed papers that intersect with other areas, such as the Internet of Things, the management of information, tracking of drugs along their supply chain, and aspects of security and privacy. They analyzed and compared both the positive and negative aspects of their papers. Finally, the authors seek to examine the concepts of blockchain in the medical area, by assessing their benefits and drawbacks and thus giving guidance to other researchers in the area. Additionally, they summarized the methods used in healthcare per application area and show their pros and cons.

- Zhao, et al. [18] presented Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems. Electronic Health Records (EHRs) are entirely controlled by hospitals instead of patients, which complicates seeking medical advice from different hospitals. Patients face a critical need to focus on the details of their own healthcare and restore management of their own medical data. The rapid development of blockchain technology promotes population healthcare, including medical records as well as patient-related data. This technology provides patients with comprehensive, immutable records, and access to EHRs free from service providers and treatment websites. In this paper, to guarantee the validity of EHRs encapsulated in blockchain, the authors presented an attribute-based signature scheme with multiple authorities, in which a patient endorses a message according to the attribute while disclosing no information other than the evidence that he has attested to it. Furthermore, there are multiple authorities without a trusted single or central one to generate and distribute public/private keys of the patient, which avoids the escrow problem and conforms to the mode of distributed data storage in the blockchain. By sharing the secret pseudorandom function seeds among authorities, this protocol resists collusion attack out of N from N −1 corrupted authorities. Under the assumption of the computational bilinear Diffie-Hellman, they also formally demonstrate that, in terms of the unforgeability and perfect privacy of the attribute-signer, this attribute-based signature scheme is secure in the random oracle model. The comparison shows the efficiency and properties between the proposed method and methods proposed in other studies.

- Azaria, et al. [19] investigated the use of blockchain for medical data access and permission management. Years of heavy regulation and bureaucratic inefficiency have slowed innovation for electronic medical records (EMRs). People now face a critical need for such innovation, as personalization and data science prompt patients to engage in the details of their healthcare and restore agency over their medical data. In this paper, the authors propose MedRec: a novel, decentralized record management system to handle EMRs, using blockchain technology. Their system gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Leveraging unique blockchain properties, MedRec manages authentication, confidentiality, accountability and data sharing- crucial considerations when handling sensitive information. A modular design integrates with providers' existing, local data storage solutions, facilitating interoperability and making our system convenient and adaptable. They incentivize medical stakeholders (researchers, public health authorities, etc.) to participate in the network as blockchain "miners". This provides them with access to aggregate, anonymized data as mining rewards, in return for sustaining and securing the network via Proof of Work. MedRec thus enables the emergence of data economics, supplying big data to empower researchers while engaging patients and providers in the choice to release metadata. The purpose of this short paper is to expose, prior to field tests, a working prototype through which we analyze and discuss our approach.

- Dwivedi, et al. [20] worked on a decentralized privacy-preserving healthcare blockchain. Medical care has become one of the most indispensable parts of human lives, leading to a dramatic increase in medical big data. To streamline the diagnosis and treatment process, healthcare professionals are now adopting Internet of Things (IoT)-based wearable technology. Recent years have witnessed billions of sensors, devices, and vehicles being connected through the Internet. One such technology, remote patient monitoring is common nowadays for the treatment and care of patients. However, these technologies also pose grave privacy risks and security concerns about the data transfer and the logging of data transactions. These security and privacy problems of medical data could result from a

delay in treatment progress, even endangering the patient's life. The authors proposed the use of a blockchain to provide secure management and analysis of healthcare big data. However, blockchains are computationally expensive, demand high bandwidth and extra computational power, and are therefore not completely suitable for most resource constrained IoT devices meant for smart cities. In this work, they tried to resolve the above-mentioned issues of using blockchain with IoT devices. They proposed a novel framework of modified blockchain models suitable for IoT devices that rely on their distributed nature and other additional privacy and security properties of the network. These additional privacy and security properties in their model are based on advanced cryptographic primitives. The solutions given here make IoT application data and transactions more secure and anonymous over a blockchain-based network.

- Tandon, et al. [21] did a thorough literature review of blockchain in healthcare. This study presents a systematic literature review (SLR) of research on blockchain applications in the healthcare domain. The review incorporated 42 articles presenting state-of-the-art knowledge on the current implications and gaps pertaining to the use of blockchain technology for improving healthcare processes. The SLR findings indicate that blockchain is being used to develop novel and advanced interventions to improve the prevalent standards of handling, sharing, and processing of medical data and personal health records. The application of blockchain technology is undergoing a conceptual evolution in the healthcare industry where it has added significant value through improved efficiency, access control, technological advancement, privacy protection, and security of data management processes. The findings also suggest that the extant limitations primarily pertain to model performance, as well as the constraints and costs associated with implementation. An integrated framework is presented to address potential areas wherein future researchers can contribute significant value, including addressing concerns regarding regulatory compliance, system architecture, and data protection. Finally, the SLR suggests that future research can facilitate the widespread deployment of blockchain applications to address critical issues related to medical diagnostics, legal compliance, avoiding fraud, and improving patient care in cases of remote monitoring or emergencies.

- Pethuru Raj, et al. [22] presented their research on blockchain technology and tools. Blockchain technology alleviates the reliance on a centralized authority to certify information integrity and ownership, as well as mediate transactions and exchange of digital assets, while enabling secure and pseudo anonymous transactions along with agreements directly between interacting parties. It possesses key properties, such as immutability, decentralization, and transparency, which potentially address pressing issues in healthcare, such as incomplete records at point of care and difficult access to patients' own health information. An efficient and effective healthcare system requires interoperability, which allows software apps and technology platforms to communicate securely and seamlessly, exchange data, and use the exchanged data across health organizations and app vendors. Unfortunately, healthcare today suffers from siloed and fragmented data, delayed communications, and disparate workflow tools caused by the lack of interoperability. Blockchain offers the opportunity to enable access to longitudinal, complete, and tamper-aware medical records that are stored in fragmented systems in a secure and pseudo anonymous fashion. This chapter focuses on the applicability of Blockchain technology in healthcare by (1) identifying potential Blockchain use cases in healthcare, (2) providing a case study that implements Blockchain technology, and (3) evaluating design considerations when applying this technology in healthcare.

- Khezr, et al. [23] did a comprehensive review of the blockchain technology in healthcare and directions for future research. One of the most important discoveries and creative developments that is playing a vital role in the professional world today is blockchain technology. Blockchain technology moves in the direction of persistent revolution and change. It is a chain of blocks that covers information and maintains trust between individuals no matter how far they are. In the last couple of years, the upsurge in blockchain technology has obliged scholars and specialists to scrutinize new ways to apply blockchain technology with a wide range of domains. The dramatic increase in blockchain technology has provided many new application opportunities, including healthcare applications. This survey provides a comprehensive review of emerging blockchain-based healthcare technologies and related applications. In this inquiry, we call attention to the open research

matters in this fast-growing field, explaining them in some details. We also show the potential of blockchain technology in revolutionizing healthcare industry.

- Agbo, et al. [24] presented a systematic review of blockchain technology in healthcare industry. Since blockchain was introduced through Bitcoin, research has been ongoing to extend its applications to non-financial use cases. Healthcare is one industry in which blockchain is expected to have significant impacts. Research in this area is relatively new but growing rapidly; so, health informatics researchers and practitioners are always struggling to keep pace with research progress in this area. This paper reports on a systematic review of the ongoing research in the application of blockchain technology in healthcare. The research methodology is based on the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) guidelines and a systematic mapping study process, in which a well-designed search protocol is used to search four scientific databases, to identify, extract and analyze all relevant publications. The review shows that a number of studies have proposed different use cases for the application of blockchain in healthcare; however, there is a lack of adequate prototype implementations and studies to characterize the effectiveness of these proposed use cases. The review further highlights the state-of-the-art in the development of blockchain applications for healthcare, their limitations and the areas for future research. To this end, therefore, there is still the need for more research to better understand, characterize and evaluate the utility of blockchain in healthcare.

- Dimiter V. Dimitrov [25] did a case report on Blockchain applications for healthcare data management. This pilot study aimed to provide an overview of the potential for blockchain technology in the healthcare system. The review covers technological topics from storing medical records in blockchains through patient personal data ownership and mobile apps for patient outreach. He performed a preliminary survey to fill the gap that exists between purely technically focused manuscripts about blockchains, on the one hand, and the literature that is mostly concerned with marketing discussions about their expected economic impact on the other hand. The findings show that new digital platforms based on

blockchains are emerging to enabling fast, simple, and seamless interaction between data providers, including patients themselves. He provided a conceptual understanding of the technical foundations of the potential for blockchain technology in healthcare, which is necessary to understand specific blockchain applications, evaluate business cases such as blockchain startups, or follow the discussion about its expected economic impacts.

- Nguyen, et al. [26] surveyed the consensus algorithms used in blockchain. Thanks to its potential in many applications, Blockchain has recently been nominated as one of the technologies exciting intense attentions. Blockchain has solved the problem of changing the original low-trust centralized ledger held by a single third-party, to a high-trust decentralized form held by different entities, or in other words, verifying nodes. The key contribution of the work of Blockchain is the consensus algorithm, which decides how agreement is made to append a new block between all nodes in the verifying network. Blockchain algorithms can be categorized into two main groups. The first group is proof-based consensus, which requires the nodes joining the verifying network to show that they are more qualified than the others to do the appending work. The second group is voting-based consensus, which requires nodes in the network to exchange their results of verifying a new block or transaction, before making the final decision. In this paper, the authors present a review of the Blockchain consensus algorithms that have been researched and that are being applied in some well-known applications at this time.

- Deepak Jain, et al. [27] set forth a deep survey of consensus algorithms in Blockchain technology. Blockchain is an immutable, transparent, public ledger that is distributed among the nodes in the network. It is a decentralized system in which transactions run on untrusted devices. To ensure equality and fairness, these transactions need to agree on some protocols. They are known as consensus algorithms. They are the core of blockchain and decide how blockchain works. Applying these algorithms, it is almost impossible for unauthorized users to crack the confidential information in the blocks. However, there are some security and performance issues that are required to be improved. In this paper, we have an overlook on various consensus algorithms, their working and where they are

applied. In addition, we have reviewed blockchain technology, its application areas, advantages, and issues.

- Sivleen Kaur, et al. [28] presented a research survey on applications of consensus protocols in blockchain technology. The concept of blockchain, widely known as virtual currencies, saw a massive surge in popularity in recent times. As far as the security of the blockchain is concerned, consensus algorithms play a vital role in the blockchain. Research has been done separately, or comparisons between a few of them have been presented previously. In this paper, the authors have discussed widely used consensus algorithms in the blockchain. The consensus protocols covered in this paper include PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), PoET (Proof of Elapsed Time), PBFT (Practical Byzantine Fault Tolerance), and PoA (Proof of Authority). For each consensus, they have reviewed the properties, applications, and performance in the blockchain.

- Md Sadek Ferdous, et al. [29] surveyed consensus algorithms in blockchain. In recent years, blockchain technology has received unparalleled attention from academia, industry, and governments all around the world. It is considered a technological breakthrough anticipated to disrupt several application domains. This has resulted in a plethora of blockchain systems for various purposes. However, many of these blockchain systems suffer from serious shortcomings related to their performance and security, which need to be addressed before any wide-scale adoption can be achieved. A crucial component of any blockchain system is its underlying consensus algorithm, which in many ways, determines its performance and security. Therefore, to address the limitations of different blockchain systems, several existing as well novel consensus algorithms have been introduced. A systematic analysis of these algorithms will help to understand how and why any particular blockchain performs the way it functions. However, the existing studies of consensus algorithms are not comprehensive. Those studies have incomplete discussions on the properties of the algorithms and fail to analyze several major blockchain consensus algorithms in terms of their scopes. This article fills this gap by analyzing a wide range of

consensus algorithms using a comprehensive taxonomy of properties and by examining the implications of different issues still prevalent in consensus algorithms in detail. The result of the analysis is presented in tabular formats, which provides a visual illustration of these algorithms in a meaningful way. The authors have also analyzed more than hundred top crypto-currencies belonging to different categories of consensus algorithms to understand their properties and to implicate different trends in these crypto-currencies. Finally, they have presented a decision tree of algorithms to be used as a tool to test the suitability of consensus algorithms under different criteria.

- Thomas McGhin, et al. [30] surveyed research challenges and opportunities in blockchain. Blockchain has a range of built-in features, such as distributed ledger, decentralized storage, authentication, security, and immutability, and has moved beyond hype to practical applications in industry sectors such as Healthcare. Blockchain applications in the healthcare sector generally require more stringent authentication, interoperability, and record sharing requirements, due to exacting legal requirements, such as Health Insurance Portability and Accountability Act of 1996 (HIPAA). Building on existing blockchain technologies, researchers in both academia and industry have started to explore applications that are geared toward healthcare use. These applications include smart contracts, fraud detection, and identity verification. Even with these improvements, there are still concerns as blockchain technology has its own specific vulnerabilities and issues that need to be addressed, such as mining incentives, mining attacks, and key management. Additionally, many of the healthcare applications have unique requirements that are not addressed by many of the blockchain experiments being explored, as highlighted in this survey paper. A number of potential research opportunities are also discussed in this paper.

- L. Soltanisehat, et al. [31] investigated Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare. Blockchain can be used to build a peer-to-peer, secure, and smart transaction system. As a horizontal technology that has changed several fields of industry, blockchain has tremendous potential to transform healthcare systems as well. In this article, a systematic review is conducted to critically

evaluate 64 articles on blockchain-based healthcare systems, published between 2016 and January 2020 in 21 conferences, 33 journals, and ten online sources. The aim of this article is to answer three main questions. First, what are the applications of blockchain in the healthcare systems, and what are the structures and challenges of applying blockchain to a specific healthcare domain? Second, what are the technical, temporal, and spatial aspects of the currently developed blockchain applications for different healthcare domain? Third, what are the future research directions in designing and implementing blockchain-based healthcare systems? Statistical facts about the technical aspects of these 64 articles show that most of the proposed blockchain-based healthcare systems use private blockchain and Ethereum platforms; furthermore, the majority of the authors are affiliated with research institutions in the USA and China. We also discuss potential future research directions, e.g., integrating the blockchain in artificial intelligence-based solutions, cloud-computing-based solutions, and parallel blockchain architecture.

- Mehdi Sookhak, et al. [32] presented a survey on Blockchain and smart contract for access control in healthcare. Emerging technologies are playing a critical role in the evolution of healthcare systems by presenting eHealth to provide high-quality services and better health to wide-range of patients. Achieving the eHealth goals highly depends on employing modern information and communication technologies (ICTs) to securely and efficiently collect and transmit electronic health records (EHRs) and make them accessible to authorized users and healthcare providers. However, the adoption of EHRs in healthcare providers puts the patients' privacy and their information security at risk of data breaches. The advent of smart contracts and blockchain technology paves a way for developing efficient EHR access control methods to support secure identification, authentication, and authorization of the clients. This paper delineates an extensive survey on the state-of-the-art blockchain-based access control methods in healthcare domain as a basis for categorizing the existing and future developments in access control area. A thematic taxonomy of the blockchain-based access control methods is also presented to recognize the security issues of the existing methods and highlight the fundamental security requirements to design a granular access control method. This paper also aims for

examining the similarities and differences of the traditional access control methods and describes some substantial and outstanding issues and challenges as further directions.

- S. A. Wright [33] puts forward the Technical and Legal Challenges for Healthcare Blockchains and Smart Contracts. The paper considers the technical and legal challenges impacting recent proposals for healthcare applications of blockchain and smart contracts. Healthcare blockchain data and actors are rather different to cryptocurrency data and actors, resulting in a different emphasis on blockchain features. Technical issues with healthcare blockchain implementation and trust are considered, as well as a variety of potential legal issues. Conclusions and recommendations are proposed for open source and standardization efforts to reduce technical and legal risks for healthcare blockchains and smart contracts.

- Tharaka Hewa, et al. [34] presented a survey on blockchain based smart contracts. Blockchain is one of the disruptive technical innovations in the recent computing paradigm. Many applications already notoriously hard and complex are fortunate to ameliorate the service with the blessings of blockchain and smart contracts. The decentralized and autonomous execution with in-built transparency of blockchain based smart contracts revolutionize most of the applications with optimum and effective functionality. The paper explores the significant applications which already benefited from the smart contracts. The authors also highlight the future potential of the blockchain based smart contracts in these applications' perspective.

- Khatoon, et al. [35] proposed a Blockchain-Based Smart Contract System for Healthcare Management related literature review. Blockchain is evolving to be a secure and reliable platform for secure data sharing in application areas such as the financial sector, supply chain management, food industry, energy sector, internet of things and healthcare. In this paper, the authors review existing literature and applications available for the healthcare system using blockchain technology. Besides, this work also proposes multiple workflows involved in the healthcare ecosystem using blockchain technology for better data

management. Different medical workflows have been designed and implemented using the Ethereum blockchain platform which involves complex medical procedures like surgery and clinical trials. This also includes accessing and managing a large amount of medical data. Within the implementation of the workflows of the medical smart contract system for healthcare management, the associated cost has been estimated for this system in terms of a feasibility study which has been comprehensively presented in this paper. This work would facilitate multiple stakeholders who are involved within the medical system to deliver better healthcare services and optimize cost.

CHAPTER 3

SMART CONTRACTS

OVERVIEW

Smart contracts are simply computer programs that are stored on a blockchain that self-execute when predetermined conditions are met. They establish trust between the end parties in an environment without any central authority. SC's working is similar to that of a vending machine. Some predetermined actions trigger a smart contract to execute itself without the intervention of a middle-man. It eliminates the need of a third-party in a transaction. SC are typically used to automate the execution of an agreement so that all participants can be immediately certain of the outcome. It enables the transactions to be carried out without any time loss. They can also automate a workflow by triggering the next action when conditions are met.

3.1 Working of a smart contract

Figure 3.1 shows a general working of the smart contracts in three simple steps:

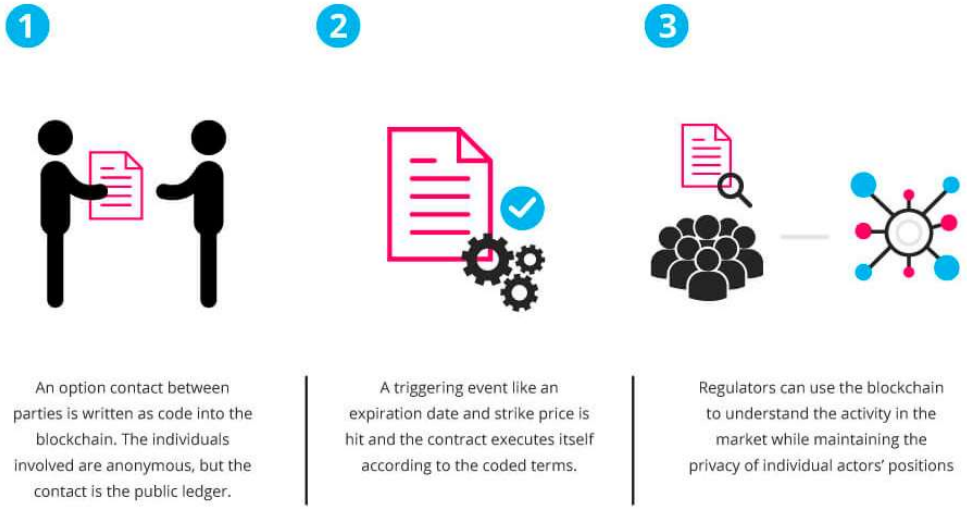

Figure 3.1: Working of a smart contract

A detailed working of SCs is described in the below steps:

Step 1: Business team and developers collaboratively decide the smart contract's desired behavior in response to certain events or conditions. Some examples of such conditions are payment authorization, shipment receipt, utility meter threshold readings etc.

Step 2: Then the complex operations and critical details are encoded using more sophisticated logic.

Step 3: A suitable smart contract writing platform is chosen.

Step 4: Developers create and test the logic internally.

Step 5: After the application is created, it is sent to another team for security testing.

Step 6: An internal team of experts that specializes in vetting smart contract security checks for loopholes.

Step 7: The contract is then deployed.

Step 8: The smart contract is configured to listen for event updates from a cryptographically secure streaming data source, once it has been deployed.

Step 9: Once it obtains the necessary combination of events, the smart contract executes.

3.2 Benefits of Smart contracts

Smart contracts can be used in a variety of fields, from healthcare to supply chain to financial services. Scs have a number of benefits. Some of them are as follows:

3.2.1 Accuracy, speed and efficiency

These three characteristics are inherently embedded into smart contracts as they are digital and automated, there is no paperwork involved. Thus, no time is wasted in correcting the errors that might have occurred while filling the documentation manually. The contract is immediately executed when a condition is met. These are the reasons why smart contracts are accurate, fast and efficient.

3.2.2 Trust and transparency

Smart contracts eliminate the need for a third party as they self-execute themselves. The data is encrypted and then exchanged among the participants. Thus, smart contracts establish trust and transparency in blockchain transactions.

3.2.3 Security

Smart contracts work on top of blockchain. It is near to impossible to hack a blockchain. Every block is linked to a block before and after it, hackers would have to change the entire chain to change a single record. In addition to that, transaction records are encrypted. Thus, smart contracts are extremely secure.

3.2.4 Savings

As mentioned above, smart contracts eliminate the third-party concept thus, it also eliminates he fees that comes with them. Smart contracts are deployed with a minimum deployment charge with is standard of a particular type of transaction. The charges are in the form of native crypto-currency of the development platform like Eth is the native crypto-currency of Ethereum platform.

3.3 Smart Contract use cases

Use cases of smart contracts can vary from sector to sector based on the requirements. Some of the use cases are mentioned in the figure 3.2 below.

Figure 3.2: Smart contract use cases

CHAPTER 4

DEPLOYMENT OF SMART CONTRACTS IN THE PROPOSED SYSTEM

OVERVIEW

Our proposed system is a blockchain-based electronic health record (EHR) sharing system. Prior to the invention of modern technology, the healthcare industry relied on a paper-based system to maintain medical records, i.e., a handwritten system. This paper-based medical record system was inefficient and unsecured. It also had to deal with redundancy because all of the hospitals where the patient went had several copies of the patient's medical records. In the present scenario, the patient's data relies on third-party-based systems which can lead to data breaching of the health records. For a long time, researchers have struggled to deal with massive amounts of data while maintaining patient privacy. Blockchain technology, on the other hand, has helped to solve some of the difficulties by offering a secure and distributed platform. The prior systems used the Proof of Work (PoW) consensus algorithm which consumes more energy but we eliminated PoW in our proposed system and our proposed system uses the Proof of stake (PoS) consensus algorithm for the consensus mechanism. Cybercriminals are continually targeting patient health records. In such circumstances, smart contracts play a critical role. Smart contracts are used to exchange and control EHR safely, preventing other parties from misusing the data. Smart Contracts provide high access to EHR records that are securely shared between pathology labs, doctors, and other entities through a distributed network. In the proposed system we used smart contracts to eliminate the third parties or middlemen. We deployed the smart contracts on the Ethereum blockchain network for which we have used ethers. Smart contracts are a set of computer programs that work as an

agreement between two parties are written in solidity language. The proposed work uses six smart contract-based system for the sharing of patient health records through a blockchain network. The paper includes three actors, a patient, a doctor, and a pathology lab in our present scenario. Pictorial working scenario of the proposed model is shown in the figure 4.1.

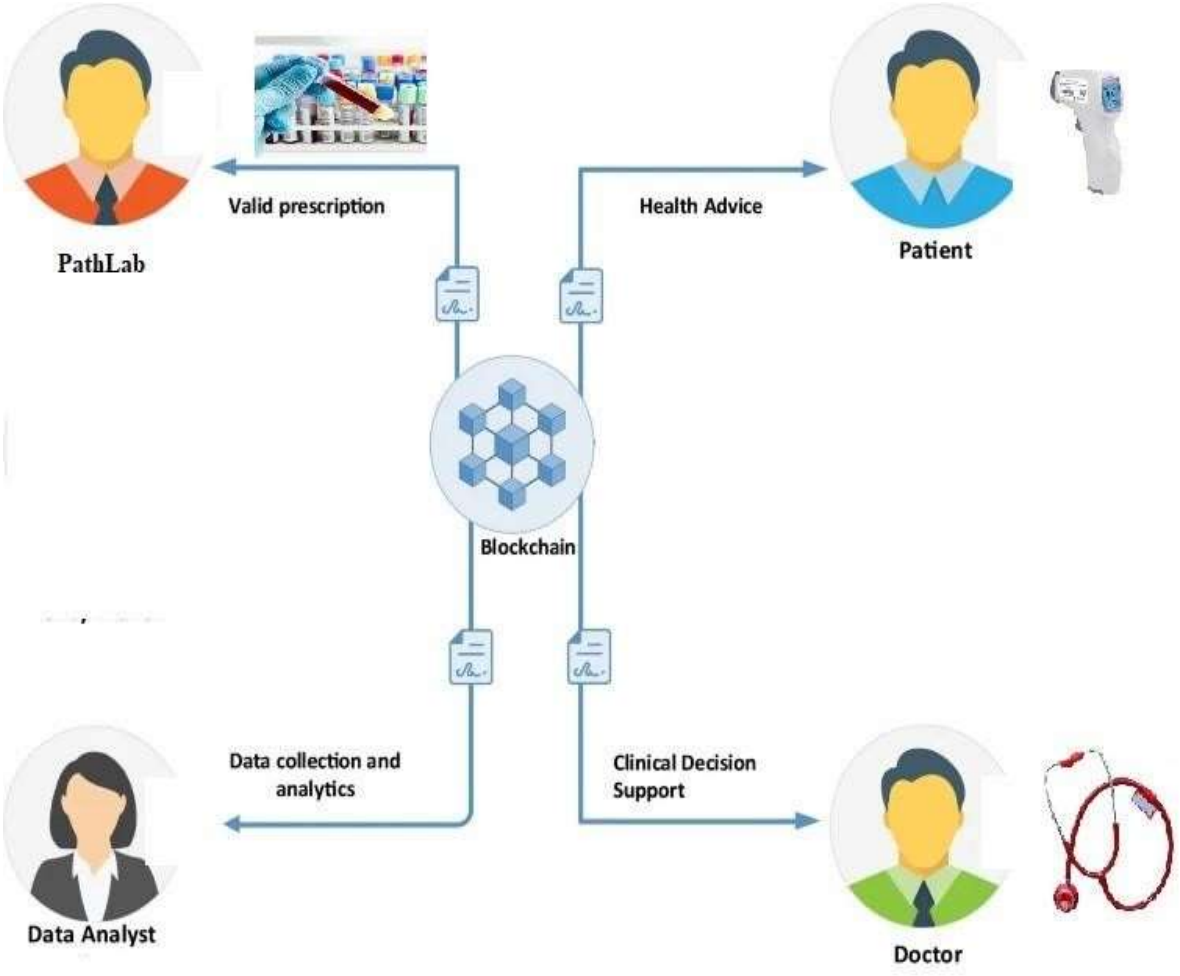

Figure 4.1: Working and entities of the proposed system

The proposed system includes a total of six smart contracts, which are discussed as follows:

4.1 Patient-to-Doctor Smart Contract

In this contract, the patient shares his or her personal information, such as medical problems, with the respective doctor. The fields which are included in this smart contract are DoctorName for the name of the respective doctor, problemDescription for outlining a patient's medical problems, Doctor field for the address of the doctor, Patient_Name for the name of the patient, Medicine_Data for the drugs recommended by the doctor, Date_of_Prescription for the prescription's date and Consult_Fee for the cost of the consultation. The owner of this contract will be a Patient. Code of the patient-to doctor sc is shown in figure 4.2.

Figure 4.2: Code of patient-to-doctor smart contract

Figure 4.3 shows the interface of patient-to-doctor smart contract.

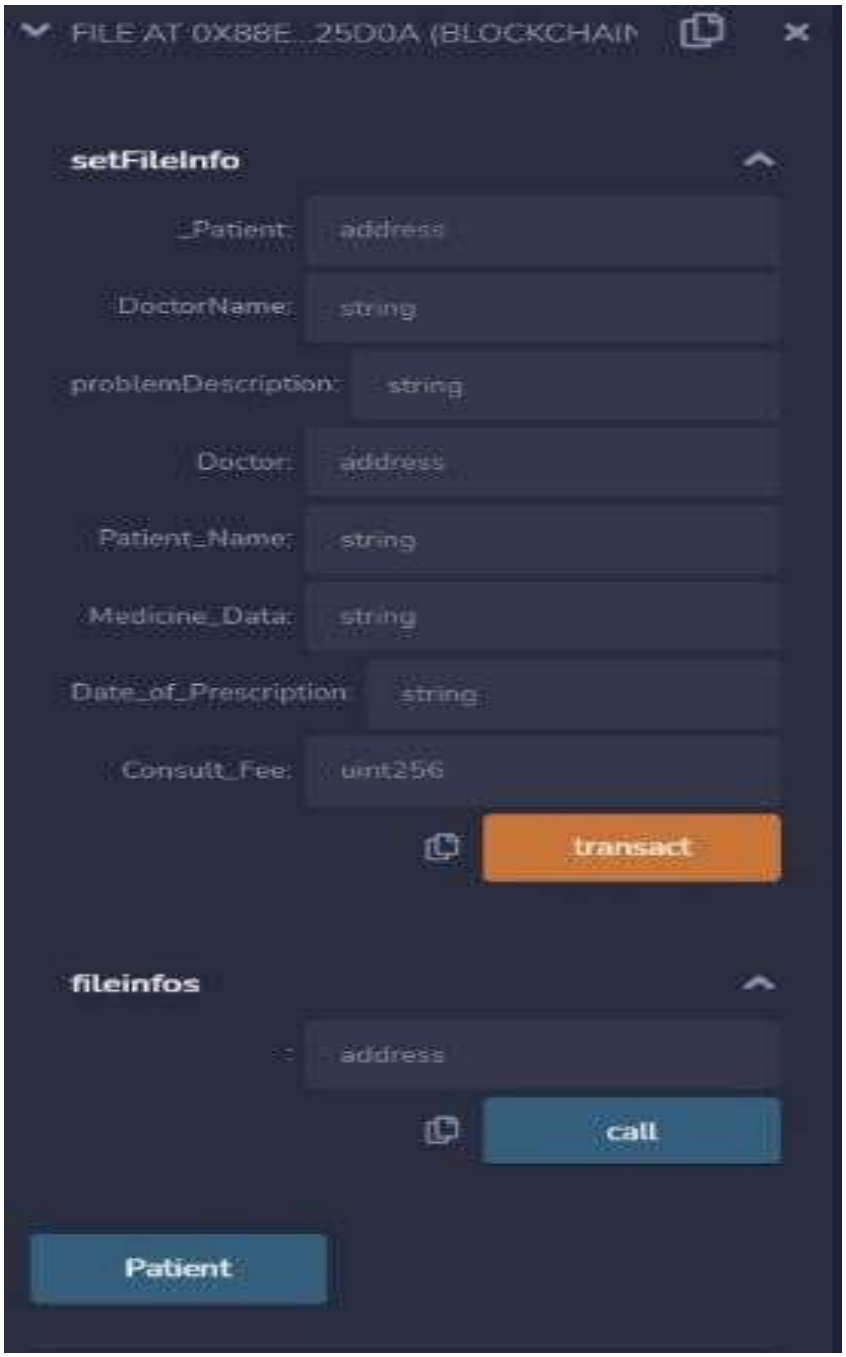

Figure 4.3: Interface of patient-to-doctor sc

The final smart contract will be formed when the code has been executed. The smart contract's existing information will be encrypted. The original data is solely accessible to the 'Patient' and the 'Doctor' but the contract is accessible to everybody. Deployment result of patient-to-doctor Smart Contract is shown in figure 4.4.

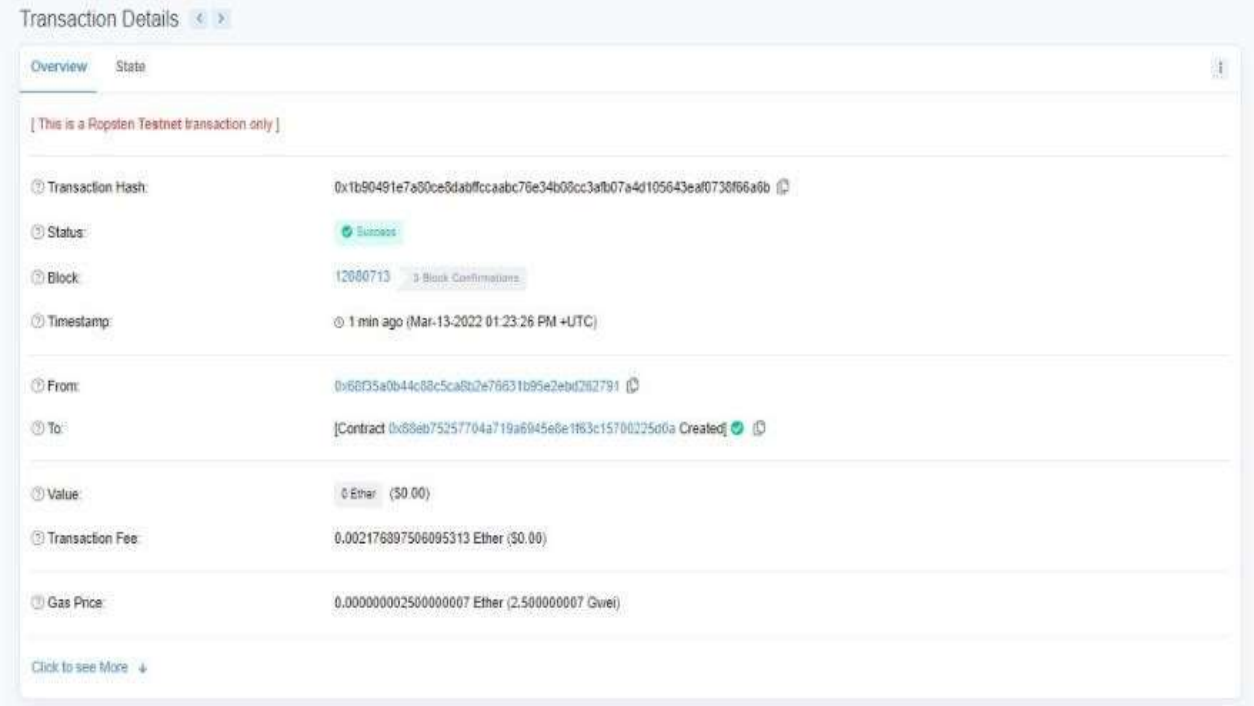

Figure 4.4: Deployment result of patient-to-doctor Smart Contract

4.2 Doctor-to-Patient Smart Contract

The doctor will share the prescription with the patient under this contract. The smart contract will have fields like DoctorName for a doctor's name, Patient for the patient's 16-bit address, Patient_Name for the patient's name, numberOfTestsToPerform for the number of health tests, testNames for the test name, and Problem_disease for the problem name. This contract will be owned by a doctor. Figure 4.5 shows the code of doctor-to-patient smart contract.

```
pragma solidity ^0.4.25;

//Declare contract having the name 'File'.
contract File{
    //Declare the structure of the contract.
    struct FileInfo{
        string DoctorName;
        address Patient;
        string Patient_Name;
        string numberOfTestsToPerform;
        string testNames;
        string Problem_disease;
    }

    address public Doctor; //Declare address of Doctor in the contract.

    //Maping the address with structure of contract.
    mapping(address => FileInfo) public fileinfos;
    //Fileinfo[] public savingmap;

    //Call a constructor for sending the data.
    constructor() public{
        Doctor = msg.sender;
        }

    //Set the permission
    modifier onlyDoctor(){
        require(msg.sender == Doctor,
    "Only Doctor can set these parameteres."
    );
    _;

    }

    //Enable the event of the contract.
    event files(string DoctorName,
        address Patient,
        string Patient_Name,
        string numberOfTestsToPerform,
        string testNames,
        string Problem_disease);

    //Call a function to set the information in the contract.
    function setFileInfo(address _Doctor, string DoctorName,
        address Patient,
        string Patient_Name,
        string numberOfTestsToPerform,
        string testNames,
        string Problem_disease)
        onlyDoctor public{

        fileinfos[_Doctor] = FileInfo( DoctorName,
         Patient,
         Patient_Name,
         numberOfTestsToPerform,
         testNames,
         Problem_disease);

        emit files(DoctorName,
         Patient,
         Patient_Name,
         numberOfTestsToPerform,
         testNames,
         Problem_disease);
    }



}
```

Figure 4.5: Code of the Doctor-to-Patient Smart Contract

Interface of Doctor-to-Patient Smart Contract is shown in figure 4.6 below.

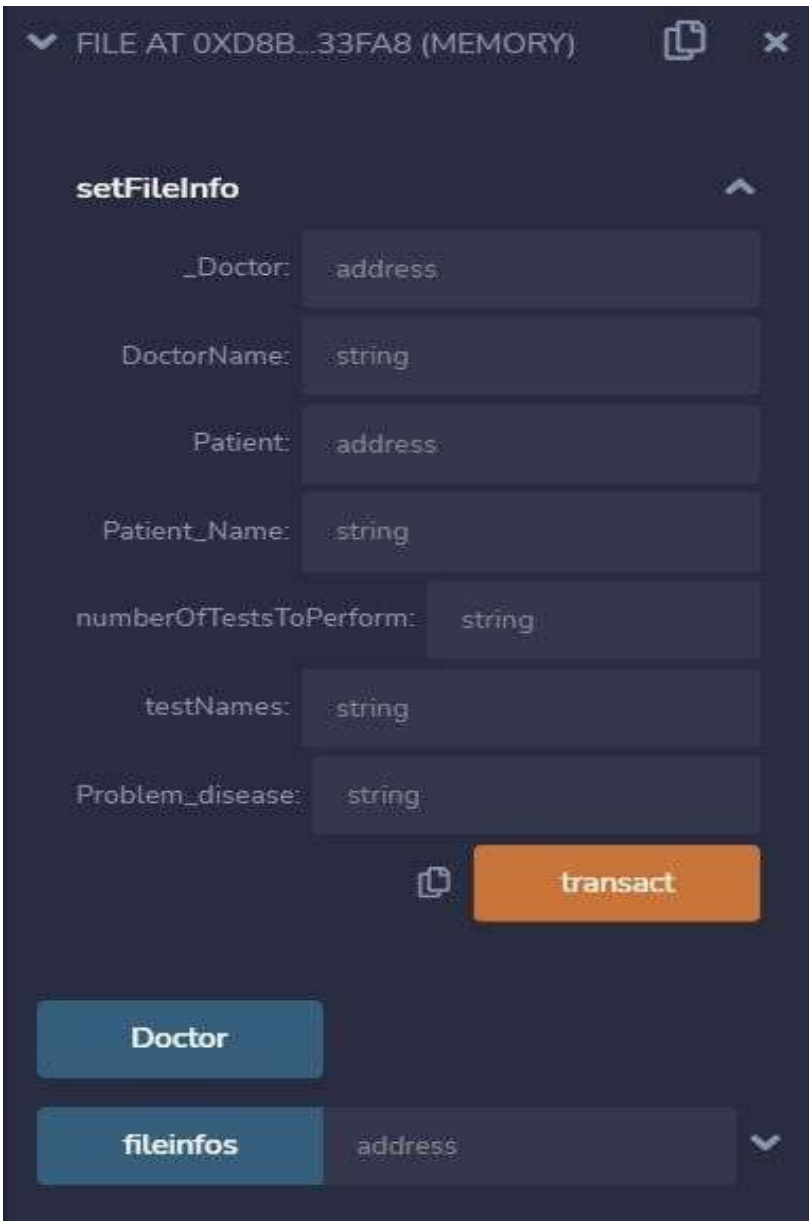

Figure 4.6: Interface of Doctor-to-Patient Smart Contract

The final smart contract will be formed when the code has been executed. The smart contract's existing information will be encrypted. The original data is solely accessible to the 'Doctor' and the 'Patient' but the contract is accessible to everybody. Figure 4.7 shows the deployment result of the Doctor-to-Patient contract.

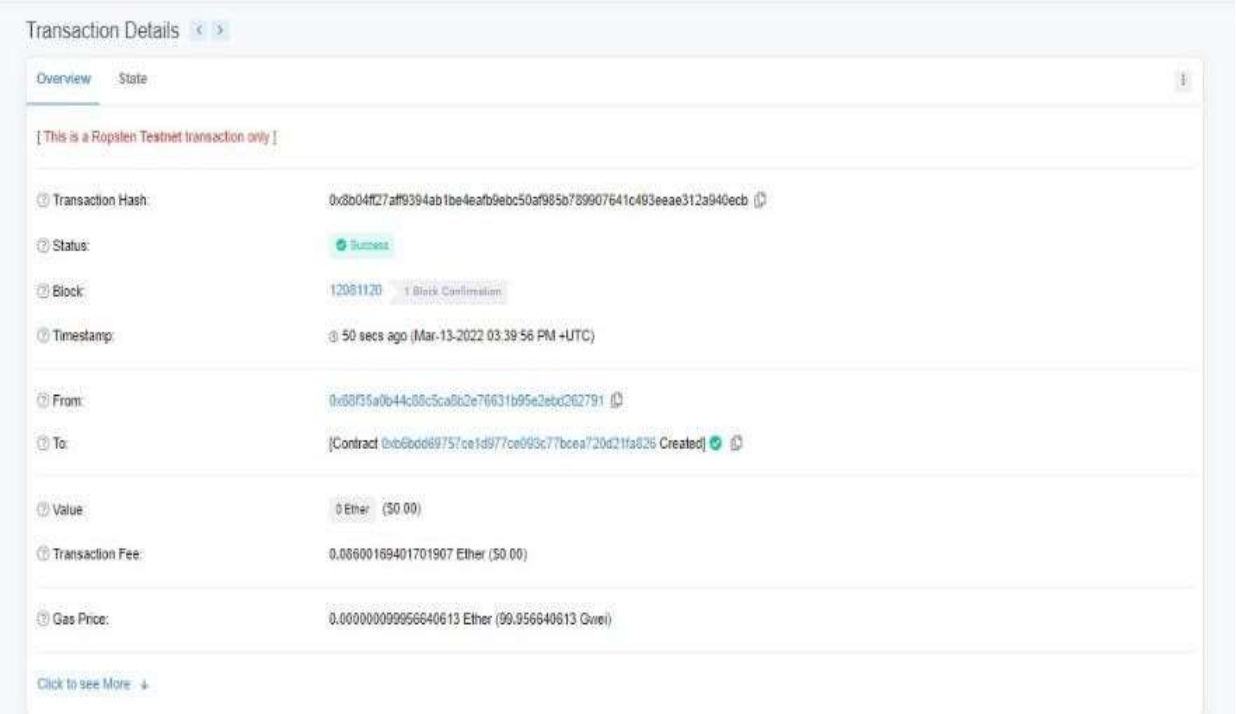

Figure 4.7: Deployment result of the Doctor-to-Patient contract

4.3 Patient-to-Lab Smart Contract

The patient agrees to share his or her medical test results with the lab under this contract. DoctorName for the name of a doctor, Lab for the address of the lab, Lab_Name for the name of the lab, Patient Name for the name of a patient, numberOfTestsToPerform for the number of health tests, testNames for the name of the test, and Problem_disease for the name of the problem will be included in the smart contract. This contract will be owned by a Patient. Figure 4.8 shows the code of the Patient-to-Lab smart contract.

```
pragma solidity ^0.4.25;

//Declare contract having the name 'File'.
contract File{
    //Declare the structure of the contract.
    struct FileInfo{
        string DoctorName;
        address Lab;
        string Lab_Name;
        string Patient_Name;
        string numberOfTestsToPerform;
        string testNames;
        string dateOfTest;
    }

    address public Patient; //Declare address of Patient in the contract.

    //Maping the address with structure of contract.
    mapping(address => FileInfo) public fileinfos;
    //Fileinfo[] public savingmap;

    //Call a constructor for sending the data.
    constructor() public{
        Patient = msg.sender;
        }

    //Set the permission
    modifier onlyDoctor(){
        require(msg.sender == Patient,
    "Only Patient can set these parameteres."
    );
    _;

    }

    //Enable the event of the contract.
    event files(string DoctorName,
        address Lab,
        string Lab_Name,
        string Patient_Name,
        string numberOfTestsToPerform,
        string testNames,
        string dateOfTest);

    //Call a function to set the information in the contract.
    function setFileInfo(address _Patient, string DoctorName,
        address Lab,
        string Lab_Name,
        string Patient_Name,
        string numberOfTestsToPerform,
        string testNames,
        string dateOfTest)

        onlyDoctor public{

        fileinfos[_Patient] = FileInfo( DoctorName, Lab, Lab_Name, Patient_Name,
numberOfTestsToPerform, testNames, dateOfTest );

        emit files(DoctorName, Lab, Lab_Name, Patient_Name,
numberOfTestsToPerform, testNames, dateOfTest);
    }



}
```

Figure 4.8: Code of Patient-to-Lab smart contract

Interface of Patient-to-Lab Smart Contract is shown in figure 4.6 below:

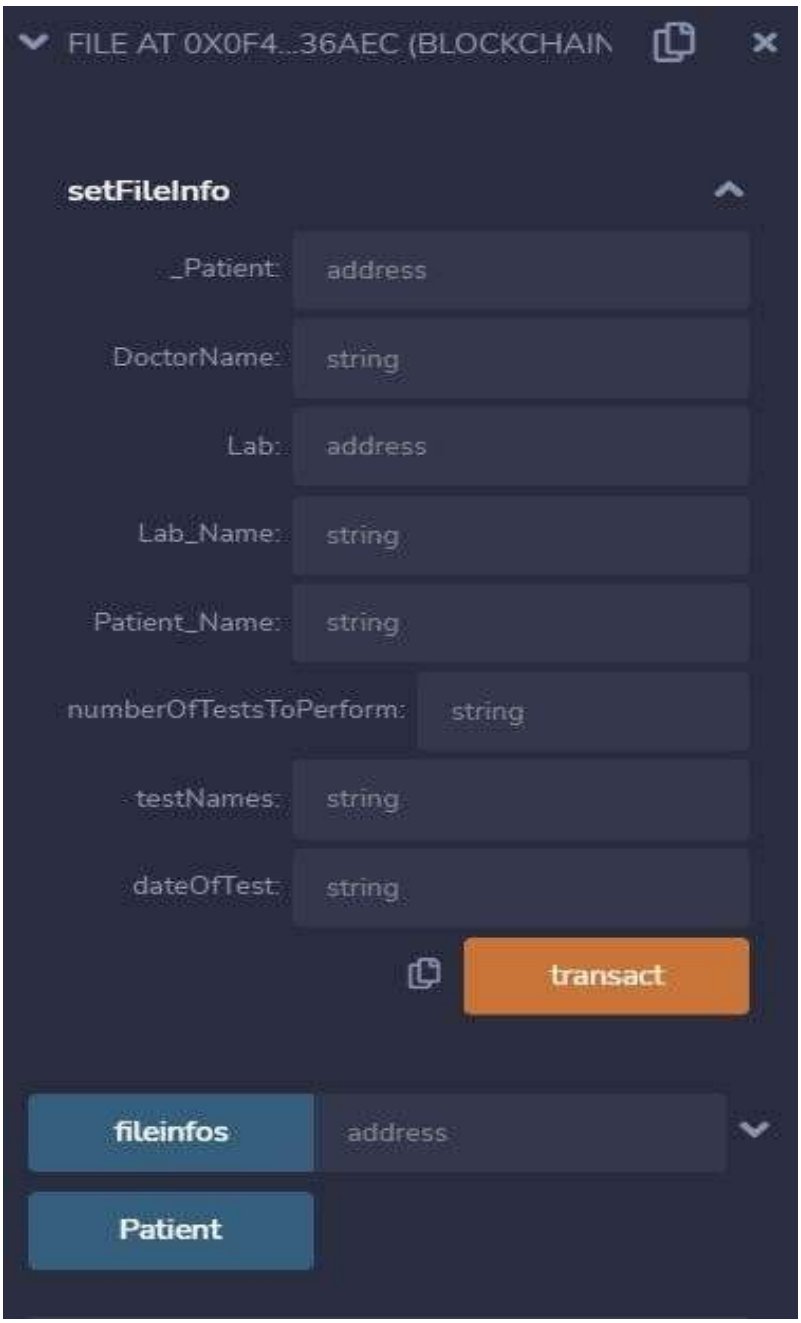

Figure 4.9: Interface of Patient-to-Lab Smart Contract

The final smart contract will be formed when the code has been executed. The smart contract's existing information will be encrypted. The original data is solely accessible to the 'Patient' and the 'Lab' but the contract is accessible to everybody. Figure 4.10 shows the deployment result of patient-to-lab contract.

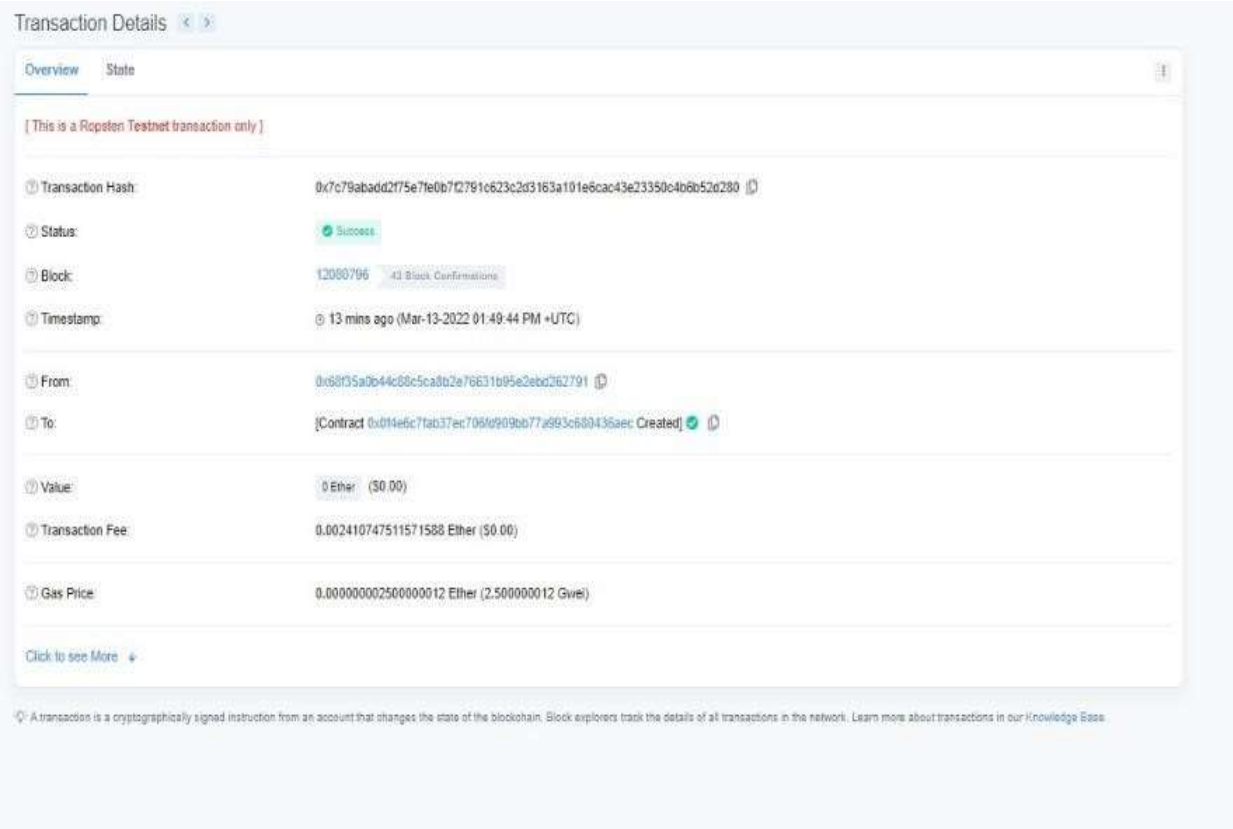

Figure 4.10: Deployment result of patient-to-lab contract

4.4 Lab-to-Patient Smart Contract

The lab will communicate the test findings with the patient under this contract. The smart contract will have fields like DoctorName for a doctor's name, Lab_Name for the lab's name, Patient_Name for a patient's name, Patient for the patient's 16-bit address, Date_of_Test for the test date, testReport_Data for the test report data, and Final testResult for the test's final results. This contract will be owned by a Lab. Figure 4.11 shows the code of the lab-to-patient smart contract.

```
pragma solidity ^0.4.25;

//Declare contract having the name 'File'.
contract File{
    //Declare the structure of the contract.
    struct FileInfo{
        string DoctorName;
        string Lab_Name;
        string Patient_Name;
        address Patient;
        string Date_of_Test;
        string testReport_Data;
        string Final_testResult;
    }

    address public Lab; //Declare address of Lab in the contract.

    //Maping the address with structure of contract.
    mapping(address => FileInfo) public fileinfos;
    //Fileinfo[] public savingmap;

    //Call a constructor for sending the data.
    constructor() public{
        Lab = msg.sender;
        }

    //Set the permission
    modifier onlyLab(){
        require(msg.sender == Lab,
    "Only Lab can set these parameteres."
    );
    _;

    }

    //Enable the event of the contract.
    event files(string DoctorName,
        string Lab_Name,
        string Patient_Name,
        address Patient,
        string Date_of_Test,
        string testReport_Data,
        string Final_testResult);

    //Call a function to set the information in the contract.
    function setFileInfo(address _Lab, string DoctorName,
        string Lab_Name,
        string Patient_Name,
        address Patient,
        string Date_of_Test,
        string testReport_Data,
        string Final_testResult)
        onlyLab public{

        fileinfos[_Lab] = FileInfo(  DoctorName,
         Lab_Name,
         Patient_Name,
         Patient,
         Date_of_Test,
         testReport_Data,
         Final_testResult);

        emit files( DoctorName,
         Lab_Name,
         Patient_Name,
         Patient,
         Date_of_Test,
         testReport_Data,
         Final_testResult);
    }


}
```

Figure 4.11: Code of the Lab-to-Patient smart contract

Interface of Lab-to-Patient smart contract is shown in the figure 4.12 below:

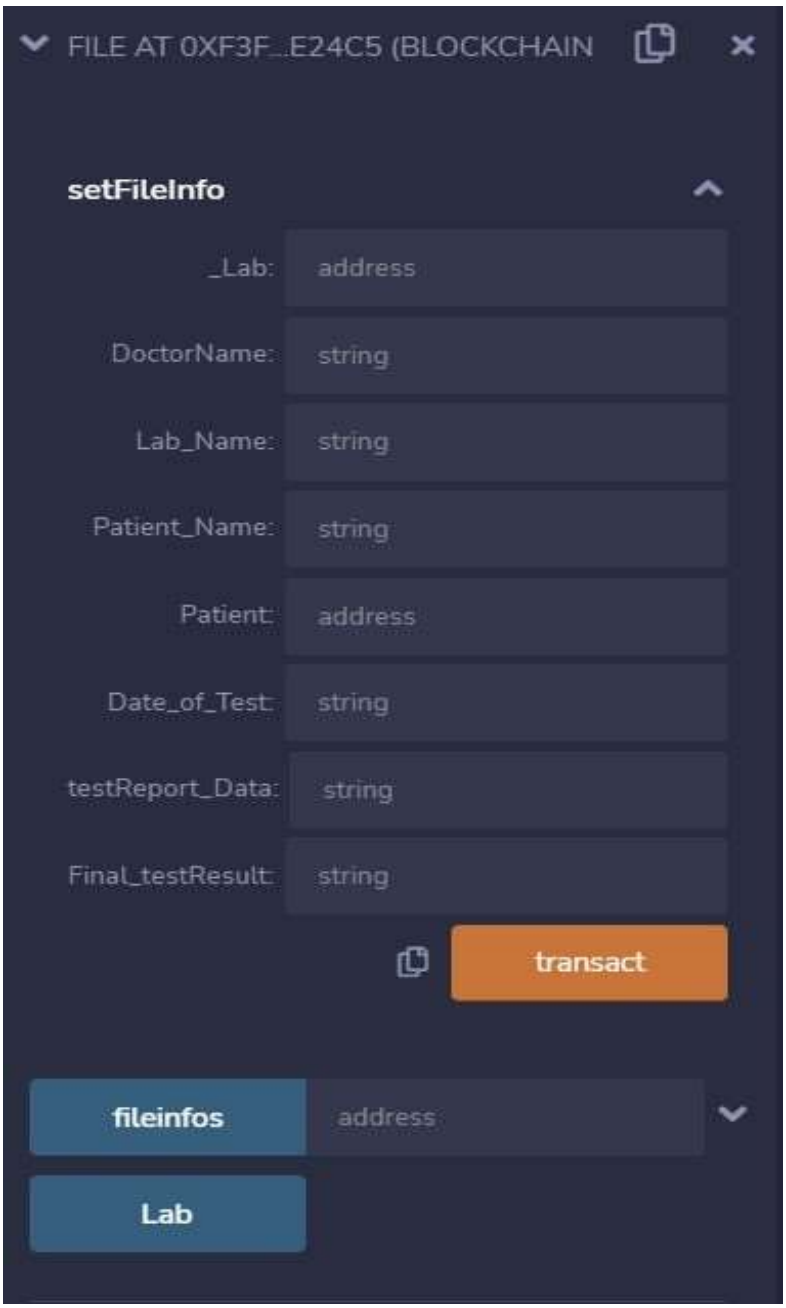

Figure 4.12: Interface of Lab-to-Patient smart contract

The final smart contract will be formed when the code has been executed. The smart contract's existing information will be encrypted. The original data is solely accessible to the 'Lab' and the 'Patient' but the contract is accessible to everybody. Figure 4.13 shows the deployment result of Lab-to-Patient contract.

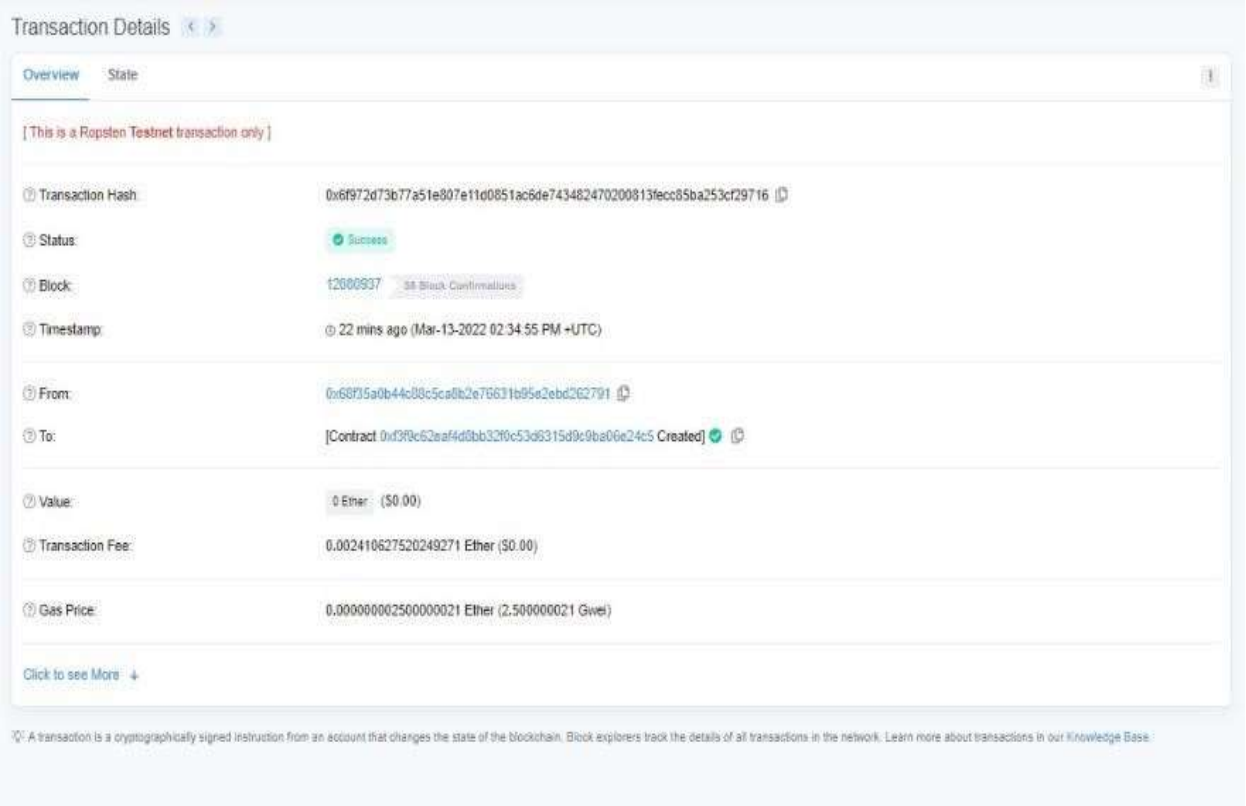

Figure 4.13: Deployment result of Lab-to-Patient contract

4.5 Patient-to-Doctor Smart Contract

The patient will share the results of the lab tests with the doctor under this contract. The smart contract will have fields like DoctorName for the doctor's name, Patient_Name for the patient's name, Doctor for the doctor's address, Lab_Name for the lab's name, lab for the lab's 16-bit address, Date_of_Test for the test's date, testReport_Data for the test report's data, and Final_testResult for the test's final results. This contract will be owned by a Patient. The code of the Patient-to-Doctor smart contract is shown in the figure 4.14.

```
pragma solidity ^0.4.25;

//Declare contract having the name 'File'.
contract File{
    //Declare the structure of the contract.
    struct FileInfo{
        string DoctorName;
        string Patient_Name;
        address Doctor;
        string Lab_Name;
        address lab;
        string Date_of_Test;
        string testReport_Data;
        string Final_testResult;
    }

    address public Patient; //Declare address of Patient in the contract.

    //Maping the address with structure of contract.
    mapping(address => FileInfo) public fileinfos;
    //Fileinfo[] public savingmap;

    //Call a constructor for sending the data.
    constructor() public{
        Patient = msg.sender;
        }

    //Set the permission
    modifier onlyPatient(){
        require(msg.sender == Patient,
    "Only Patient can set these parameteres."
    );
    _;

    }

    //Enable the event of the contract.
    event files(string DoctorName,
        string Patient_Name,
        address Doctor,
        string Lab_Name,
        address lab,
        string Date_of_Test,
        string testReport_Data,
        string Final_testResult);
```

```
    //Call a function to set the information in the contract.
    function setFileInfo(address _Patient, string DoctorName,
        string Patient_Name,
        address Doctor,
        string Lab_Name,
        address lab,
        string Date_of_Test,
        string testReport_Data,
        string Final_testResult)
        onlyPatient public{

        fileinfos[_Patient] = FileInfo( DoctorName,
         Patient_Name,
         Doctor,
         Lab_Name,
         lab,
         Date_of_Test,
         testReport_Data,
         Final_testResult);

        emit files(DoctorName,
         Patient_Name,
         Doctor,
         Lab_Name,
         lab,
         Date_of_Test,
         testReport_Data,
         Final_testResult);
    }
```

Figure 4.14: Code of the Patient-to-Doctor smart contract

Interface of patient-to-doctor smart contract is shown in the figure 4.15 below:

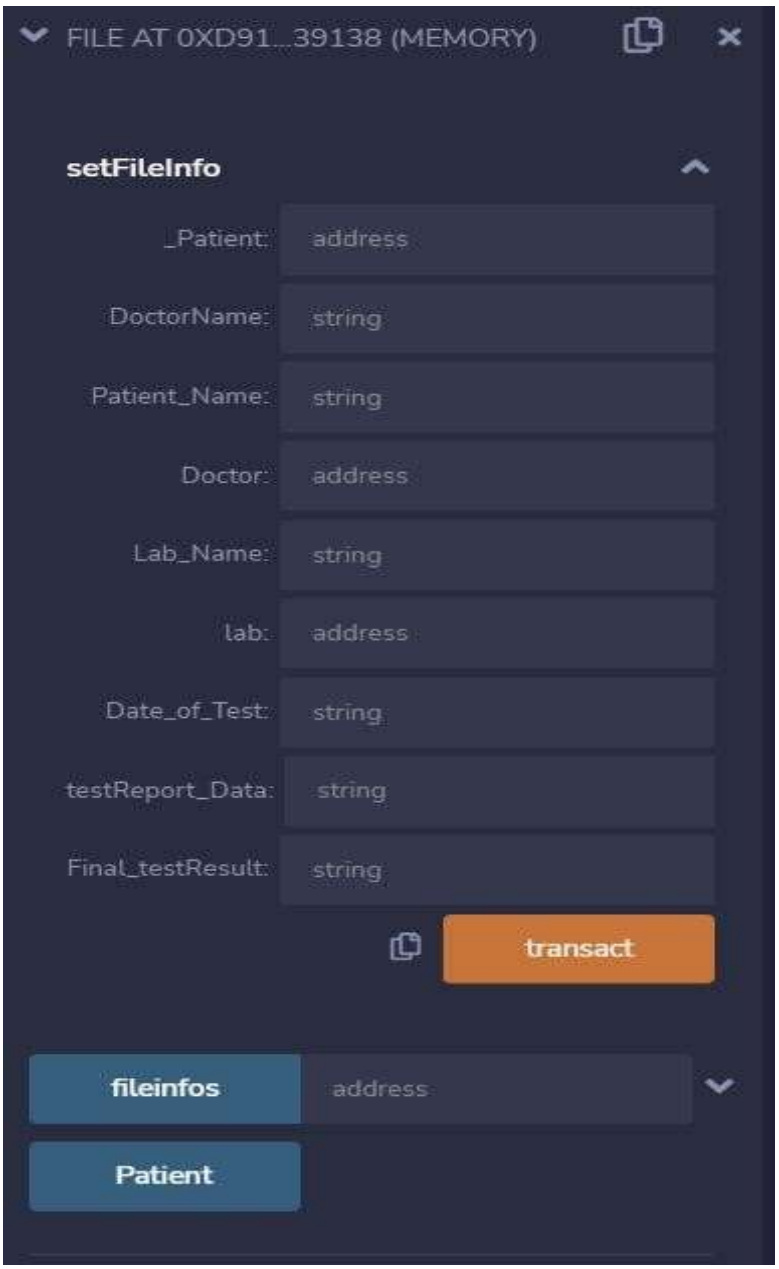

Figure 4.15: Interface of patient-to-doctor smart contract

The final smart contract will be formed when the code has been executed. The smart contract's existing information will be encrypted. The original data is only accessible to the 'Patient' and the 'Doctor,' but the contract is accessible to everybody. Figure 4.16 shows the deployment of the Patient-to-Doctor smart contract.

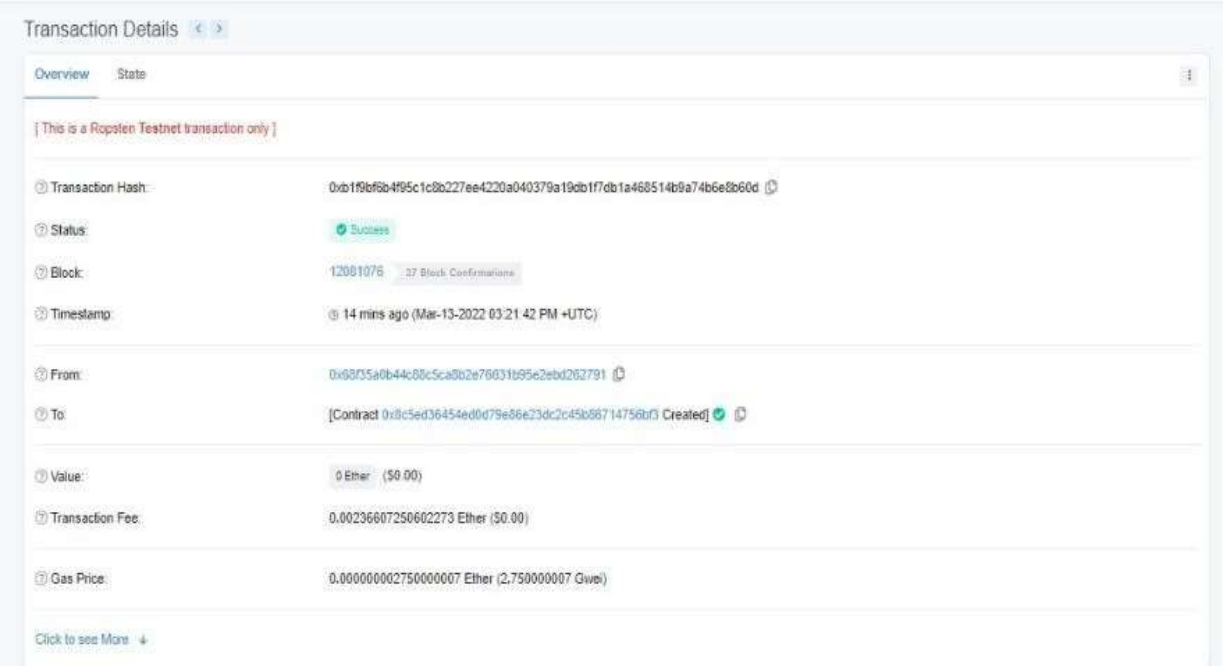

Figure 4.16: Deployment of the Patient-to-Doctor smart contract

4.6 Doctor-to-Patient Smart Contract

The doctor will share the prescription with the patient under this contract. The smart contract will have fields like DoctorName for a doctor's name, Patient for a patient's 16-bit address, Patient_Name is a placeholder for a patient's name, Medicine_Prescriptions for prescribed medications, testResult for the results of the test, Problem_disease for the health issues of a patient, Date_of_Prescription for the date of the prescription and the Consult_Fee for the consultation cost. The owner of this contract will be a doctor. Figure 4.17 shows the code of the Doctor-to-Patient smart contract.

```
pragma solidity ^0.4.25;

//Declare contract having the name 'File'.
contract File{
    //Declare the structure of the contract.
    struct FileInfo{
        string DoctorName;
        address Patient;
        string Patient_Name;
        string Medicine_Prescription;
        string testResult;
        string Problem_disease;
        string Date_of_Prescription;
        uint Consult_Fee;
    }

    address public Doctor; //Declare address of Doctor in the contract.

    //Maping the address with structure of contract.
    mapping(address => FileInfo) public fileinfos;
    //Fileinfo[] public savingmap;

    //Call a constructor for sending the data.
    constructor() public{
        Doctor = msg.sender;
        }

    //Set the permission
    modifier onlyDoctor(){
        require(msg.sender == Doctor,
    "Only Doctor can set these parameteres."
    );
    _;

    }

    //Enable the event of the contract.
    event files(string DoctorName, address Patient, string Patient_Name, string
Medicine_Prescription, string Problem_disease, string Date_of_Prescription,
string testResult, uint Consult_Fee);

    //Call a function to set the information in the contract.
    function setFileInfo(address _Doctor, string DoctorName, address Patient,
string Patient_Name, string Medicine_Prescription, string Problem_disease, string
Date_of_Prescription, string testResult, uint Consult_Fee)
        onlyDoctor public{

        fileinfos[_Doctor] = FileInfo(DoctorName, Patient,  Patient_Name,
Medicine_Prescription, Problem_disease, Date_of_Prescription,  testResult,
Consult_Fee );

        emit files(DoctorName, Patient, Patient_Name, Medicine_Prescription,
Problem_disease, Date_of_Prescription, testResult, Consult_Fee);
    }


}
```

Figure 4.17: Code for Doctor-to-Patient smart contract

Interface of Doctor-to-Patient smart contract is shown in the figure 4.18 below:

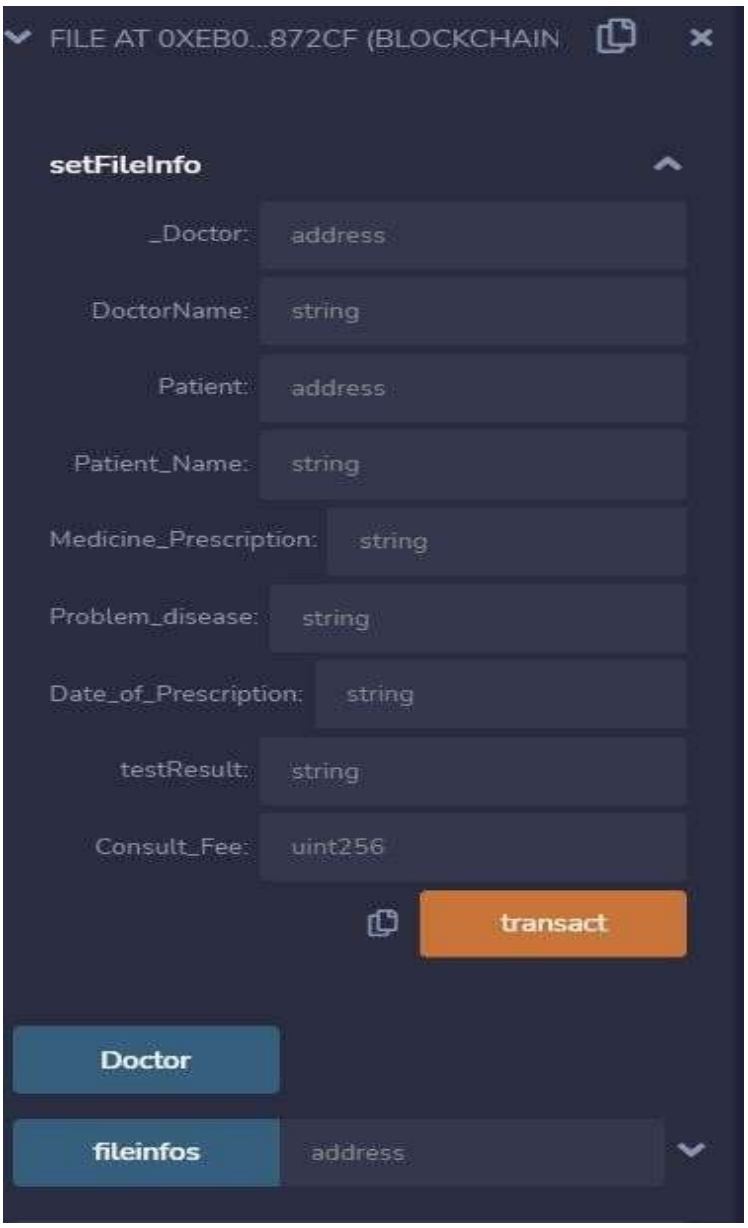

Figure 4.18: Interface of Doctor-to-Patient smart contract

The final smart contract will be formed when the code has been executed. The smart contract's existing information will be encrypted. The original data is solely accessible to the 'Doctor' and the 'Patient' but the contract is accessible to everybody. Figure 4.19 shows the deployment of the Doctor-to-Patient smart contract.

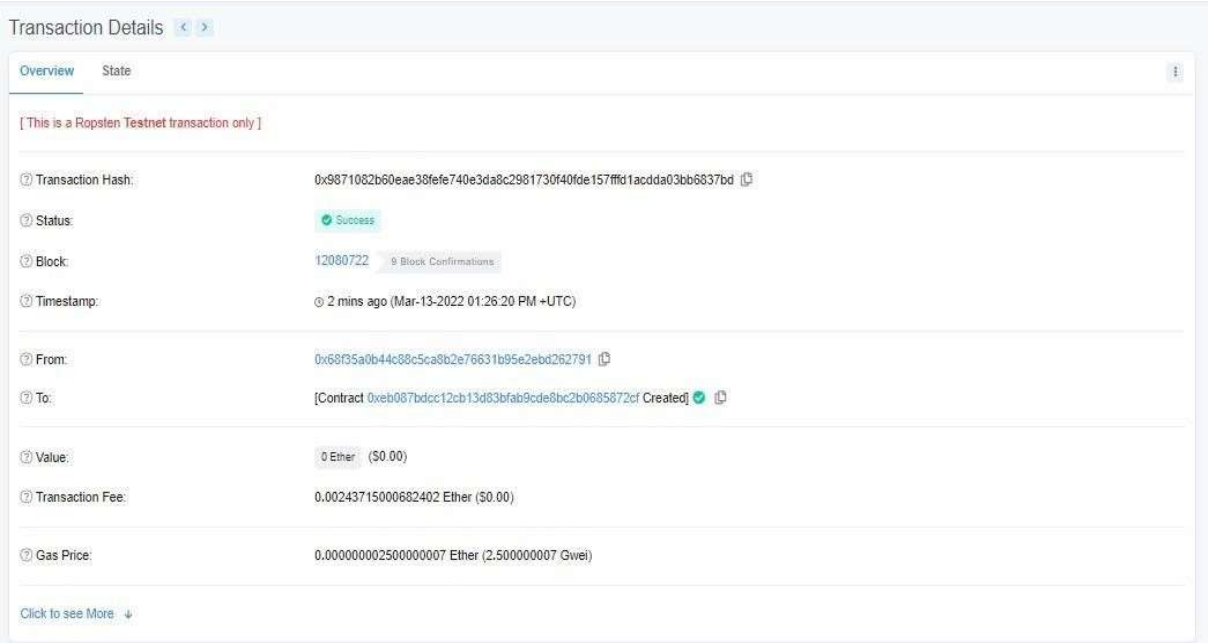

Figure 4.19: Deployment of the Doctor-to-Patient smart contract

CHAPTER 5

SUSTAINABILITY DEVELOPMENT GOALS

OVERVIEW

The Sustainable Development Goals (SDGs) are a collection of 17 distinct objectives set by the UN General Assembly in 2015. The SDGs represent a universal call to action to end poverty, protect the planet, and ensure that all people enjoy peace and prosperity. The SDGs are specifically designed to engage companies to tackle the world's most pressing challenges. These challenges include poverty and inequalities, climate change and environmental degradation, aging societies and population growth, economic volatility, political instability, and societal upheaval. Moreover, the SDGs entail profound implications for corporate strategic decision-making.

5.1 The 17 Sustainability development goals

For the past decades, the only purpose of the businesses was to reach their financial objectives. Yet, to meet the SDGs, companies often need to reconsider their business conduct and reinvent the purpose of their organizations, set alternative non-financial goals, and adopt strategy approaches that allow the inclusion of various stakeholder sets. These 17 goals are discussed in this chapter.

5.1.1 No Poverty

End poverty in all its forms everywhere. This goal consists of many targets like, by 2030, eradicate extreme poverty for all people everywhere, reduce at least by half the

proportion of men, women and children of all ages living in poverty in all its dimensions according to national definitions, implement nationally appropriate social protection systems and measures for all, including floors, and achieve substantial coverage of the poor and the vulnerable and many more.

5.1.2 Zero Hunger

The targets in this goal are to end hunger, achieve food security, improve food nutrition and promote sustainable agriculture.

5.1.3 Good health and well-being

Good health and well-being goal strives to ensure healthy lives and promote well-being for all at all ages. It states many targets like reduce the global maternal mortality ratio to less than 70 per 100,000 live births by 2030.

5.1.4 Quality education

This goal in SDGs aims to achieve the inclusive and equitable quality education and promote lifelong learning opportunities for all.

5.1.5 Gender equality

The main motto here is to achieve gender equality and empower all women and girls. It aims to end all forms of discrimination, violence and harmful practices against women and girls everywhere.

5.1.6 Clean water and sanitation

Water is the most basic necessity of every human-being. Through this goal UN strives to achieve availability and sustainability management of water and sanitation for all and for everyone around the globe.

5.1.7 Affordable and clean energy

It is to ensure access to affordable, reliable, sustainable and modern energy for all. It strives to increase substantially the share of renewable energy in the global energy mix and double the global rate of improvement in energy efficiency by the year 2030.

5.1.8 Decent work and economic growth

It promotes sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all.

5.1.9 Industry, innovation and infrastructure

This goal means, build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation. One of its main targets is to develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all.

5.1.10 Reduced inequalities

Its tag line is, reduce inequality within and among countries. UN targets to empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion or economic or other status by the year 2030.

5.1.11 Sustainable cities and communities

This goal emphasizes on making cities and human settlements inclusive, safer, resilient and sustainable. The main aim is to ensure access for all to adequate, safe and affordable housing and basic services and upgrade slums by the year 2030.

5.1.12 Responsible consumption and production

This aim encloses sustainable consumptions and production patterns. Top target is to Implement the 10-year framework of programs on sustainable consumption and production, all countries taking action, with developed countries taking the lead, taking into account the development and capabilities of developing countries

5.1.13 Climate action

The need of the hour is to take urgent action to combat climate change and its impact or else there wouldn't be a planet to call ours soon.

5.1.14 Life below water

This goal aims to spread awareness to conserve and sustainable use the oceans, seas and marine resources for sustainable development.

5.1.15 Life on land

The tag line of this goal states that protect, restore and promote sustainable use of terrestrial ecosystems, sustainable manage forests, combat desertification, and halt and reserve land degradation and halt biodiversity loss.

5.1.16 Peace, justice and strong institutions

This goal promotes peaceful and inclusive societies for sustainable development, provide access to justice for all and built effective, accountable and inclusive institutions at all levels.

5.1.17 Partnerships for the goals

It strengthens the means of implementation and revitalize the global partnership for sustainable development. The main task is to Strengthen domestic resource mobilization,

including through international support to developing countries, to improve domestic capacity for tax and other revenue collection.

5.2 The SDGs promoted in this work

In the proposed system, two SDGs have been promoted which are stated and described below in this section.

5.2.1 Industry, innovation and infrastructure

This is the 9th SDG that aims to Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all. Through the proposed model we aim to develop a system that is free of any third-party involvement which leads to the minimization of handling fees. It is more secure and faster than the current models.

5.2.2 Climate action

This is the 13th SDG provided by the UN. It suggests to take urgent action to combat climate change and its impact. The proposed system uses PoS consensus algorithm instead of PoW consensus algorithm. PoW requires dedicated servers and a huge amount of computing which causes extreme effects on the environment. But, PoS requires way less computation and thus, comparatively more environment friendly than the PoW consensus algorithm.

CHAPTER 6

CONCLUSION

The major goal of this research paper is to show how blockchain technology can be used to create a more efficient and secure health record sharing system, as well as how blockchain can be used to address the challenging process of handling sensitive patient data using smart contracts. Blockchain is a well-known technology that has aided in the resolution of a wide range of challenges in a variety of industries. It's a technology that's tamper-proof, transparent, and secure. Blockchain is a potentially powerful and revolutionary technology since it reduces risk, eliminates fraud, and promotes transparency in a scalable manner for a wide range of applications. It's a distributed ledger of records that's verified by a global network of computers. The records are governed by a large community rather than a single central authority, and no single person has control over the records. This technology uses consensus mechanisms for security purposes. The data is encrypted using extremely advanced algos, and only the legal owner has access to it. The consensus algorithms which are used in blockchain are Proof of Work (PoW), Proof of Stake (PoS), Proof of Burn, etc.

In Blockchain it’s nearly impossible to tamper with the data as it is stored in a block and each block of the blockchain contains its Hash value and the Hash value of the previous block so, when anyone tries to change the data or tamper with a block then the block will be rejected because its Hash value will change. Blockchain is used in a wide range of areas such as supply chain, healthcare, cryptocurrency exchange, banking, law enforcement, voting, internet of things, real estate, digital Ids, etc. In the healthcare field, blockchain technology ensures safe access to patient records. The security of a patient's data is a key problem. The growing number of ransom assaults

in the healthcare industry is another motive to design a safe system. Blockchain technology provides a safe platform for storing patient medical information in the form of electronic health records (EHR) without involving third parties. The suggested approach guarantees that lab findings are quickly shared with patients and practitioners, as well as it prevents data breaching. The proposed system talks about the use of blockchain and smart contracts in the healthcare industry.

CHAPTER-7

FUTURE WORK

The future work will be focused on the development of a proper GUI system to enhance the present system and the possibility of switching from Ethereum blockchain to Hyperledger. Currently, the proposed system is between doctor-patient-lab which can be further extended to pharmacies. This work can be extended even more if we add more elements to the system like care-givers.

REFERENCES

[1] Maher Alharby, Amjad Aldweesh, Aad vad Moorsel, "Blockchain-based Smart Contracts: A systematic mapping study of academic research", AIRCC's International Journal of Computer Science and Information Technology, vol 9, no 5, 2017, pp: 151-164, DoI: 10.1109/ICCBB.2018.8756390.

[2] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE International Congress on Big Data, 2017, DoI: 10.1109/BigDataCongress.2017.85.

[3] Simanta Shekhar Sarmah, Understanding Blockchain Technology, Computer Science and Engineering, vol. 8, no. 2, 2018, pp: 23-29, DoI: 10.5923/j.computer.20180802.02.

[4] Zibin Zheng and Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang,"Blockchain challenges and opportunities: a survey", Int. J. Web and Grid Services, vol. 14, no. 4, pp: 352–375, DoI: DoI: 10.1504/IJWGS.2018.095647.

[5] N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," 2018 12th International Conference on Open-Source Systems and Technologies (ICOSST), 2018, pp. 54-63, doi: 10.1109/ICOSST.2018.8632190.

[6] Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, Khan RA. "Healthcare Data Breaches: Insights and Implications. Healthcare (Basel)", vol. 8 issue 2. 2021 doi: 10.3390/healthcare8020133.

[7] Vinodhini Mani, Prakash Manickam, Youseef Alotaibi, Saleh Alghamdi, Osamah Ibrahim Khalaf, "Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records", Electronics, vol. 10, issue 23, pp.: 3003, 2021, DoI: https://doi.org/10.3390/electronics10233003

[8] Bahar Houtan; Abdelhakim Senhaji Hafid; Dimitrios Makrakis, "A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare", IEEE Access, vol. 8, pp. 90478–90494, 2020, DoI: 10.1109/ACCESS.2020.2994090.

[9] Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T., "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring". J. Med. Syst. vol. 42, article.130, 2018, DoI: 10.1007/s10916-018-0982-x

[10] X. Zhu and Y. Badr, ''Identity management systems for the Internet of Things: A survey towards blockchain solutions,'' Sensors, vol. 18, no. 12, pp. 1-18, 2018. DoI: https://doi.org/10.3390/s1812421

[11] Naresh Chandra, Vipin Kumar and Arun Kumar Tripathi, "A Deep Investigation on Blockchain Network based on Platforms and Consensus Algorithms", International Journal of Advanced Science and Technology, vol. 29, issue 8s, pp. 3614 – 3629, 2020.

[12] M. Quinn, J. Forman, M. Harrod, S. Winter, K. E. Fowler, S. L. Krein, A. Gupta, S. Saint, H. Singh, and V. Chopra, ''Electronic health records, communication, and data sharing: Challenges and opportunities for improving the diagnostic process,'' Diagnosis, vol. 6, no. 3, pp. 241–248, Aug. 2019.

[13] Apoorv Jain, Arun Kumar Tripathi, Naresh Chandra and P. Chinnasamy, "Smart Contract enabled Online Examination System Based in Blockchain Network", IEEE International Conference on Computer Communication and Informatics (ICCCI), 27-29 Jan. 2021

[14] T. McGhin, K.-K.-R. Choo, C. Z. Liu, and D. He, ''Blockchain in healthcare applications: Research challenges and opportunities,'' J. Netw. Comput. Appl., vol. 135, pp. 62–75, 2019.

[15] I. Berges, J. Bermudez, and A. Illarramendi, ''Toward semantic interoperability of electronic health records'' IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 3, pp. 424–431, 2012, DoI: 10.1109/TITB.2011.2180917.

[16] Ajay Kumar Shrivastava, Akash Rajak, Chetan and Arun Kumar Tripathi, "A Decentralized way to

Store and Authenticate Educational Documents on Private Blockchain", IEEE International Conference ICICT-2019, 27-28 September 2019, DoI: 10.1109/ICICT46931.2019.8977633.
[17] De Aguiar EJ, Faic¸al BS, Krishnamachari B, Ueyama J., "A survey of blockchain-based strategies for healthcare", ACM Comput Surv (CSUR), vol. 53, issue, 2, pp. :1–27, 2021, DoI: https://doi.org/10.1145/3376915
[18] Guo, R.; Shi, H.; Zhao, Q.; Zheng, D., "Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems", IEEE Access 2018, vol. 6, pp: 11676 – 11686, DoI: 10.1109/ACCESS.2018.2801266
[19] Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec, "Using blockchain for medical data access and permission management", International Conference on Open and Big Data (OBD), Vienna, Austria, pp. 25–30, 2016, DoI: 10.1109/OBD.2016.11
[20] Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT", Sensors, vol. 19, issue 2, 2019, DoI: https://doi.org/10.3390/s19020326
[21] Tandon, Anushree & Dhir, Amandeep & Islam, A.K.M. Najmul and Mäntymäki, Matti, "Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Computers in Industry", vol. 122, 2020, pp: 1-22, DoI: 10.1016/j.compind.2020.103290.
[22] Pethuru Raj and Ganesh Chandra Deka; "Blockchain Technology: Platforms, Tools and Use Cases, Advances in Computers, vol. 111, 2019, ISBN: 978-0128138526.
[23] Khezr, Seyednima, Md Moniruzzaman, Abdulsalam Yassine, and Rachid Benlamri. "Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research" Applied Sciences, vol. 9, no. 9, 2019, DoI: https://doi.org/10.3390/app9091736
[24] Agbo, Cornelius C., Qusay H. Mahmoud, and J. M. Eklund. "Blockchain Technology in Healthcare: A Systematic Review", Healthcare vol. 7, no. 2, 2019, DoI: https://doi.org/10.3390/healthcare7020056
[25] Dimiter V. Dimitrov, "Blockchain applications for healthcare data management. Healthcare Inform" Res. vol. 25, issue 1, pp: 51–56, 2019, DoI: 10.4258/hir.2019.25.1.51.
[26] Nguyen, Truong & Kim, Kyungbaek. "A survey about consensus algorithms used in Blockchain. Journal of Information Processing Systems", vol. 14, no. 1, pp. 101-128, DoI: 10.3745/JIPS.01.0024.
[27] Sharma, Kapil and Deepak Jain, "Consensus Algorithms in Blockchain Technology: A Survey", International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 6-8 July 2019, pp: 1-7, DOI: 10.1109/ICCCNT45670.2019.8944509
[28] Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, Jayaprakash Kar, "A Research Survey on Applications of Consensus Protocols in Blockchain", Security and Communication Networks, vol. 2021, pp. 1- 22, 2021, DoI: https://doi.org/10.1155/2021/6693731
[29] Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad A. Hoque, Alan Colman, "Blockchain Consensus Algorithms: A Survey; IEEE: New York, NY, USA, 2020, available at: http://arxiv.org/abs/2001.07091
[30] Thomas McGhin, Kim-Kwang Raymond Choo, Charles Zhechao Liu, Debiao He, "Blockchain in healthcare applications: Research challenges and opportunities", Journal of Network and Computer Applications, vol. 135, pp. 62-75,2019, DoI: https://doi.org/10.1016/j.jnca.2019.02.027.
[31] L. Soltanisehat, R. Alizadeh, H. Hao and K. R. Choo, "Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review," in IEEE Transactions on Engineering Management, pp: 1-16, 2020, DoI: 10.1109/TEM.2020.3013507.
[32] Mehdi Sookhak, Mohammad Reza Jabbarpour, Nader Sohrabi Safa, F. Richard Yu, Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues, Journal of Network and Computer Applications, vol. 178, 2021, pp: 1-22, DoI: https://doi.org/10.1016/j.jnca.2020.102950.
[33] S. A. Wright, "Technical and Legal Challenges for Healthcare Blockchains and Smart Contracts", ITU Kaleidoscope: ICT for Health: Networks, Standards and Innovation (ITU K), 2019, pp. 1-9, DoI: 10.23919/ITUK48006.2019.8996146.
[34] Tharaka Hewa, Mika Ylianttila, Madhusanka Liyanage, "Survey on blockchain based smart contracts: Applications, opportunities and challenges", Journal of Network and Computer Applications, vol. 177, 2021, pp:1-39, DoI: https://doi.org/10.1016/j.jnca.2020.102857.
[35] Khatoon, Asma. "A Blockchain-Based Smart Contract System for Healthcare

Management" Electronics, vol. 9, no. 1, pp: 1-23, 2020 DoI: https://doi.org/10.3390/electronics9010094