sustainability

MDPI

Article

Blockchain Technology and Artificial Intelligence Based Decentralized Access Control Model to Enable Secure Interoperability for Healthcare

Sumit Kumar Rana [1], Sanjeev Kumar Rana [1], Kashif Nisar [2,3], Ag Asri Ag Ibrahim [3,*], Arun Kumar Rana [4], Nitin Goyal [5] and Paras Chawla [6]

[1] Department of Computer Science and Engineering, Maharishi Markandeshwar (Deemed to Be University), Ambala 133207, India; sumitrana.cse@gmail.com (S.K.R.); dr.sanjeevrana@mmumullana.org (S.K.R.)
[2] College of Computer Science and Information Systems, Institute of Business Management, Korangi Creek Road, Karachi 75190, Sindh, Pakistan; kashif@ums.edu.my
[3] Faculty of Computing and Informatics, University Malaysia Sabah, Jalan UMS, Kota Kinabalu 88400, Malaysia
[4] Panipat Institute of Engineering and Technology, Samalkha 132101, India; ranaarun1.ece@piet.co.in
[5] Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura 140401, India; nitin.goyal@chitkara.edu.in
[6] Associate Dean-Curriculum Development (DAA), Chandigarh University, Mohali 140110, India; drparaschawla.ece@cumail.in
* Correspondence: awgasri@ums.edu.my

Abstract: Healthcare, one of the most important industries, is data-oriented, but most of the research in this industry focuses on incorporating the internet of things (IoT) or connecting medical equipment. Very few researchers are looking at the data generated in the healthcare industry. Data are very important tools in this competitive world, as they can be integrated with artificial intelligence (AI) to promote sustainability. Healthcare data include the health records of patients, drug-related data, clinical trials data, data from various medical equipment, etc. Most of the data management processes are manual, time-consuming, and error-prone. Even then, different healthcare industries do not trust each other to share and collaborate on data. Distributed ledger technology is being used for innovations in different sectors including healthcare. This technology can be incorporated to maintain and exchange data between different healthcare organizations, such as hospitals, insurance companies, laboratories, pharmacies, etc. Various attributes of this technology, such as its immutability, transparency, provenance etc., can bring trust and security to the domain of the healthcare sector. In this paper, a decentralized access control model is proposed to enable the secure interoperability of different healthcare organizations. This model uses the Ethereum blockchain for its implementation. This model interfaces patients, doctors, chemists, and insurance companies, empowering the consistent and secure exchange of data. The major concerns are maintaining a history of the transactions and avoiding unauthorized updates in health records. Any transaction that changes the state of the data is reflected in the distributed ledger and can be easily traced with this model. Only authorized entities can access their respective data. Even the administrator will not be able to modify any medical records.

Keywords: blockchain; content identifier; digitalization; artificial intelligence; blockchain

Citation: Rana, S.K.; Rana, S.K.; Nisar, K.; Ag Ibrahim, A.A.; Rana, A.K.; Goyal, N.; Chawla, P. Blockchain Technology and Artificial Intelligence Based Decentralized Access Control Model to Enable Secure Interoperability for Healthcare. *Sustainability* **2022**, *14*, 9471. https://doi.org/10.3390/su14159471

Academic Editors: Kamalakanta Muduli, Rakesh Raut, Balkrishna Eknath Narkhede and Himanshu Shee

Received: 12 February 2022
Accepted: 17 March 2022
Published: 2 August 2022

1. Introduction

One of the most important pillars of society is its healthcare sector, because it's related to the wellbeing and lives of human beings. This sector needs innovative ideas that can advance the standard of healthy life by providing solutions to different health-related issues.

The healthcare sector generates large amounts of data that are utilized by different stakeholders of the system, as shown in Figure 1. These data are very sensitive and avoiding sharing them over a public network is very critical. The exchange of patient data is necessary

because sometimes doctors at different physical locations need to take a combined decision or want an opinion from another expert. This process should confirm that communicating entities are receiving up-to-date information. This exchange should take place in a secure and authenticated process [1]. The security and privacy of the data are the primary concerns for any health data exchange. Furthermore, severe interoperability concerns plague this field on a regular basis. Extensive, trustworthy, and healthy engagements between the parties involved are required for such clinical data transfers.

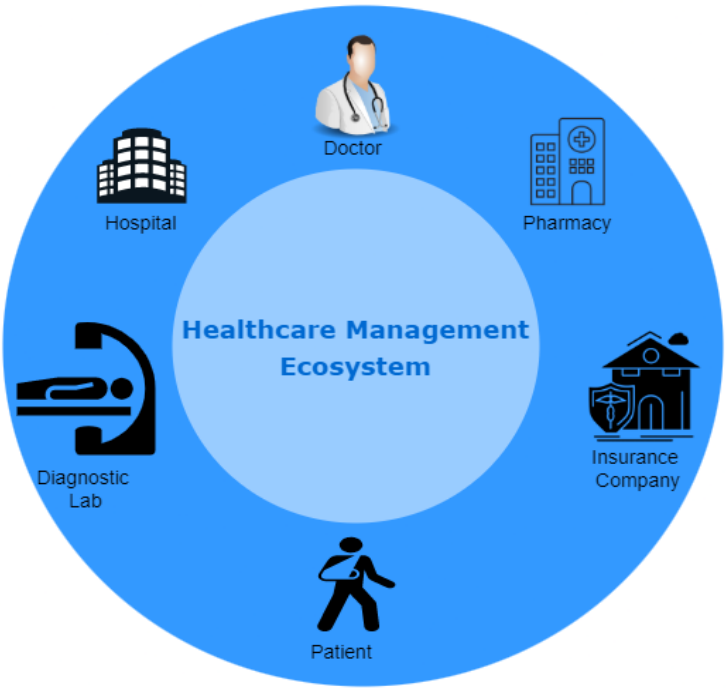

Figure 1. Different Stakeholders in the healthcare management ecosystem.

The innovations and latest breakthroughs in technology have made it easy to witness improvements in the health sector domain. The medical sector's current capabilities may be enhanced further by using the most cutting-edge and innovative computer technology. This cutting-edge computer technology can aid doctors and medical professionals in the early detection of a variety of ailments [2]. These powerful computer technologies can also greatly increase the accuracy of detecting illnesses at their early stages. Various developing and innovative computer technologies are already being applied with spectacular outcomes in other industries, among them blockchain technology, IoT, artificial intelligence, etc.

Because of the centralized nature of the current system, security remains a source for worry. As a result, security may be provided via a new and growing technology called blockchains [3–6]. By identifying the limitations of existing security procedures, blockchain technology may be used to improve security. It is a decentralized point-to-point network that removes the need for an intermediary in transactions and communication [7]. All of the transactions are self-contained and separate from one another. Blockchains are the technology that underpins the popular and ground breaking notion of cryptocurrencies. Everyone has access to blockchains, which are a publicly distributed ledger system [8–10].

The blocks in the chain consist of data, a hash of the preceding block, and the hash of all the transactions [11–13]. It is divided into two sections: the header and the transaction information. The block's information is contained in the header. The "timestamp" keeps track of when the block was generated. The "difficulty level" determines how difficult mining a block will be [14]. The hash of all the transactions of the current block is represented by "Merkle tree root", and "NONCE" is the answer to the proof-of-work algorithm's mathematical problem.

Motivation, Objective, and Contributions

In this article, the application of an emerging technology in the healthcare field is discussed. In healthcare, blockchain technology can help with drug traceability, medical record management, and other issues. The healthcare sector is facing lot of difficulties due to the vulnerability of healthcare data to security threats such as assaults on truthfulness, confidentiality, and availability. As a result, blockchain technology may be used in healthcare to improve the sector's capacities, while also ensuring the confidentiality of patients' information. However, the introduction of new and evolving technologies in any industry can result in a number of concerns and obstacles. So, identifying such concerns and obstacles is critical, particularly in the healthcare industry, where human lives are closely linked. The feasibility of adopting blockchains in the healthcare sector is investigated in this article. Contributions made by this article are listed below.

- Various issues in the healthcare industry are explored and the benefits of integrating blockchain technology in the healthcare industry are discussed.
- A blockchain-supported, decentralized access control solution is proposed and implemented. Moreover, it can be tailored for implementation on other blockchain frameworks.
- The execution costs of various functions of smart contracts with slow, standard, and fast executions are compared.
- The proof-of-authority consensus procedure is employed in the proposed paradigm. A few selected nodes will function as validators that will have the authority to validate the transactions. Because only preselected validator nodes will validate the transaction, the time necessary to create a block is predictable and smaller than the time required to generate a block using the proof-of-work process.

This paper is structured as follows: In Section 2, a literature study is performed to find out insights into the domain of healthcare. Section 3 elaborates on the advantages of employing blockchain technology in the healthcare industry. Section 4 describes the blockchain-supported proposed architecture. The methodology for the proposed work is described in Section 5. In Section 6, the implementation results and analysis are shown. In Section 7, research implications are discussed. Finally, the article is concluded in Section 8.

2. Literature Study

Legacy systems in the medical and healthcare fields often only exchange healthcare data within the organization but not outside it. Nonetheless, data suggest that combining these networks for linked and improved healthcare has a number of significant benefits, prompting health informatics academics to demand for interconnections across diverse organizations. Multi-organizational data sharing is an important challenge, since it necessitates that private data provided by a healthcare firm be freely accessible to other organizations. Distributed ledger technology is redefining the process of data management and governance in the domain of the medical system because of different features of blockchains, such as their immutability, provenance, transparency etc. The blockchain is the key to many contemporary advances in the healthcare business [15].

New options for the administration of medical information, as well as for the ease for people to have ownership and share their respective medical data, are opening up. Any data-driven company has to ensure the security, storage, transactions, and easy integration of their data. This is especially true in the medical field, where distributed ledger technology offers the ability to tackle these important concerns in a very effective way [16].

There are multiple levels to distributed ledger technology in healthcare breakthroughs, including its data sources and stakeholders. Gordon and Catalini completed their debate on the use of distributed ledger technology to make the complete system patient-centric, not institution-oriented. They looked at how distributed ledger technology could improve the healthcare industry by providing decentralized access rights, entity identification throughout the system, and data immutableness [17].

Hyperledger Fabric was used as a blockchain framework for the management of healthcare digital assets. The authors acquired the required medical data with the help of mobile phone devices. Their aim was to store the medical data on the blockchain using the Hyperledger framework [18].

Authors explored distributed ledger technology as a solution to efficiently handle the medically related data. They examined the benefits and limitations of employing this technology in the medical domain. The benefits include privacy of patient data, security, and transparency of data movements. There are also some limitations, such as the integration of this emerging technology with traditional infrastructure being costly and difficult. As this is an emerging field, there are fewer skilled professionals. The authors also investigated how this technology can be used in combination with cloud technology for medical data while maintaining security [19].

The authors proposed a model for the resolution of the restrictions of distributed ledger technology. This model was implemented using the Hyperledger framework for the management of patient-oriented medical data [20].

The authors introduced two security techniques for the networks after a survey of the healthcare domain. They also promoted distributed ledger technology as the best solution for privacy and security preservation [21].

MedChain was a system proposed by the authors to exchange healthcare data by utilizing distributed ledger technology and p-2-p networks. The authors created the system to collect patient data from IoT sensors and other mobile apps, Voice over IP (VoIP), and WiMAX as well as healthcare data provided by medical examinations [22].

Khezr et al. explored how blockchain technology might be used to tackle numerous challenges in the healthcare management system. They discussed the latest research on medical data utilizing this technology, as well as several potential medical use cases in which this technology might play a key part in streamlining the process. They've also presented a networking protocol based IoMT delivery system [23].

In addition to conducting a survey on healthcare difficulties, the authors examined various challenges related to healthcare. These issues were the security of the medical data of the patients, the transparency of the communications between different entities, the accessibility of the data, etc., and the authors discussed blockchain-based solutions to address these issues [24].

Breaches of patient information such as names, addresses, and other personal information were common, according to the authors. They proposed a blockchain-based system for dealing with medical records. The major resolution of their work was to evaluate the performance of their system in order to assess how well their suggested framework handled the demands of patients, physicians, and third parties [25].

The authors proposed a book chapter in which they examined several healthcare blockchain application cases. They have emphasized the need for a blockchain-based healthcare system and how this technology may help with medical system design [26].

The authors discussed how distributed ledger technology might help the medical industry by simplifying procedures. They have indicated in their study that keeping healthcare records is critical, and that technology has the ability to decrease data loss and avoid data fabrication by safeguarding information [27].

Jamil et al. explored medication restrictions and how to standardize pharmaceuticals by utilizing blockchain technology. They have underlined the difficulty in detecting fake pharmaceuticals in their study and advocated blockchain as a method for detecting counterfeits [28].

Using a blockchain and a microscope sensor, Lee and Yang developed a fingernail analysis management system. Human nails are one of a kind and represent a person's physiological makeup. They employed minuscule sensors to capture nail pictures and pre-processing methods to produce clear photos in their research. The performance of a feature extraction technique was monitored using a deep neural network. Blockchain

technology was employed to safeguard user data, offer security and privacy, and track and record any changes in the system via the ledger [29].

The authors investigated a thorough analysis of existing blockchain applications in the domain of healthcare. Their research demonstrated that distributed ledger technology can be the perfect fit for many medical applications. They also suggested that better knowledge of this technology can open up new research directions in the healthcare domain. Healthcare innovation has been delayed by inefficiency and stringent restrictions [30].

The regulatory difficulties that produce inefficiencies in the EMR system were explored by the authors. They have presented a distributed-ledger-supported solution to handle massive amounts of medical data. They have exhibited a new and inventive way for gaining access to medical records that includes a fair audit log system. Using distributed ledger technology, MedRec allowed patients and clinicians to exchange medical data with other parties. They provide incentives for people such as researchers and other health professionals to engage in the mining process [31].

The authors talked about the use of distributed ledger technology to solve a variety of issues in the medical domain. Multiple issues related to the privacy and security of medical data can be tackled with this technology. They went on to say that by creating blockchain-supported applications, they can more effectively handle healthcare challenges [32].

The authors highlighted the use cases of distributed ledger technology in the domain of the healthcare industry. They have identified the various hurdles in the adoption of distributed ledger technology. They also developed smart contracts for the management of medical systems [33].

The authors advocated distributed ledger technology as the safest way to manage data related to the healthcare domain. As per their survey, due to hacker motivations and secrecy violations, digital safety was a serious concern. It was achievable in the eHealth field, by applying several rules wherein the management of patients' data must adhere to several regulations while staying accessible to officially authorized healthcare practitioners. Most people were aware of distributed ledger technology because of its most popular application in the payment industry, Bitcoin [34].

According to Nofer et al., the distributed ledger system has various advantages that include the protection of personal and confidential information, removing intermediates, etc. Unlike centralized networks, the functioning of the network remains even if individual nodes fail. It enhances confidence since the intermediary or other network members' trustworthiness is not appraised by people. Data security was also supported by the absence of intermediaries, because the involvement of intermediaries also leads to data security breaches. By utilizing distributed ledger technology, intermediaries may become obsolete, significantly boosting the user's safety [35].

The security and confidentiality problems of personal information management were highlighted in a paper by the MIT Media Lab, which emphasized all blockchain technology deployments. The worth of data processing is that it is safe in the sense that it cannot be tampered with. Data privacy and protection were another facet of data security. Enigma, for example, is a decentralized computer platform with assured anonymity and a blockchain innovation. Enigma's mission is to allow inventors to create peer-to-peer decentralized applications that are "privacy by design" without the need for intermediaries. The blockchain is an "operating system" for safe collaborative tasks performed by nodes in a network. Enigma is an extension to distributed ledger technology because processing and data storage are completed outside the blockchain [36].

The blockchain was described as a safe house for processing all types of delicate data. It defined the distributed ledger as a decentralized system. A large number of business difficulties can be solved by this technology. Encryption safeguards the records in a blockchain transaction, and each block is backward-connected to previous blocks by the hashing technique. Transactions were validated with different consensus algorithms. Blockchains will eventually achieve transparency, allowing each user to trace transactions at any moment. A smart contract is a secure method of preventing intervention by intermediaries. Ethereum is

a public blockchain which is powered by smart contracts. This aids creators in the creation of markets for the long-term movement of money based on instructions issued in the past. Decentralization, immutability, rapid transfers, payment, and confirmation in real time are the major aspects of blockchains [37].

Authors took advantage of cloud technology to swiftly detect user behaviors and harvest data from the source. They developed and executed a model for the gathering and authentication of data origins, by embedding historical data into distributed ledger transactions. Data gathering and data validation from historical information were the three main steps of the proposed model. According to performance evaluation findings, ProvChain improved security for cloud-based storage systems which includes customer confidentiality and minimal overhead dependability, [38].

The current healthcare industry has a number of issues. Patients' health records contain sensitive and important information. Without a proper access control policy, these records can be misused by unauthorized users. In conventional approaches, proving the ownership of data is a tough task. Secondly, it is also discovered that the "names" were not those of real people, and a considerable number of names had different spellings. There are also some concerns with health insurance coverage. To begin with, exchanging information with many stakeholders is a time-consuming procedure. In the traditional approach, tracing a fraudulent insurance claim is extremely difficult. As participants add tainted, inadequately maintained, and falsified substances, the illegal drug market contributes significantly to the production of phony and fraudulent medications. Drug traceability is difficult because there aren't enough technological and business solutions that provide proper traceability and provenance. Confidentiality is another issue with the traditional systems. The data are visible to any unauthorized user once they get into the centralized databases of the traditional systems. These issues can be resolved by integrating blockchain technology into the healthcare industry. Some of the benefits are discussed in the next section.

3. Benefits of Employing Blockchain Technology for Healthcare

Blockchain technology supports a decentralized network where no one is the sole owner of the system [39]. The layered architecture of blockchain-technology-supported applications is shown in Figure 2. At the application-layer level, the front end developed in HTML, React, Javascript, etc. is used to access the system [40]. All the logic is written in the form of smart contracts at the access layer. Then, consensus is achieved via different algorithms such as proof of work (PoW), proof of stake (PoS), etc., at the consensus layer [41–45]. It supports a peer-to-peer system at the networking level. Data are present in the form of transactions and blocks at the data layer.

Multiple benefits can be achieved by different stakeholders from distributed ledger technology, as shown in Figure 3. A healthcare application can spur the construction of a new type of "smart" healthcare worker which can produce personalized treatment plans [46–49]. All the stakeholders can access the information with proper access controls in a decentralized peer-to-peer network. The following are the benefits of employing this technology in the healthcare industry:

1. **Towards complete and interoperable health records**

It can help address the interoperability issue in a way better than current solutions because of its enhanced safety and capacity to develop belief between entities [50–54].

2. **Smart contracts for better coordination**

This technology can gather the data from all the entities automatically with proper permissions from the owners of the data. Then every entity can collaborate with other entities for more constructive outcomes by using smart contacts [55–59].

3. **More successfully detecting fraud**

If any patient applies for a fake insurance claim, then these claims can be detected with the help of smart contracts [60].

4. **Improving the correctness of the provider directory**

Every entity has some unique address that can be used by decentralized consensus mechanisms to make it easier for insurance companies and insurers to modify entries. Confidentiality is maintained by using cryptography in blockchain systems. Every entity has an associated public and private key pair. This pair is cryptographically connected, and it is not technically feasible to produce one key from another key of the pair [61,62].

5. **More client-centric to simplify it**

Using a blockchain to provide an easier-to-access, more complete collection of medical information might provide relief and satisfaction from what has become an invasive and sometimes disappointing application process [63].

6. **Assisting in the development of a dynamic insurer–client relationship**

A dynamic relationship can be built between insurer and client. All the interaction between the entities can be managed with the help of smart contracts [64,65].

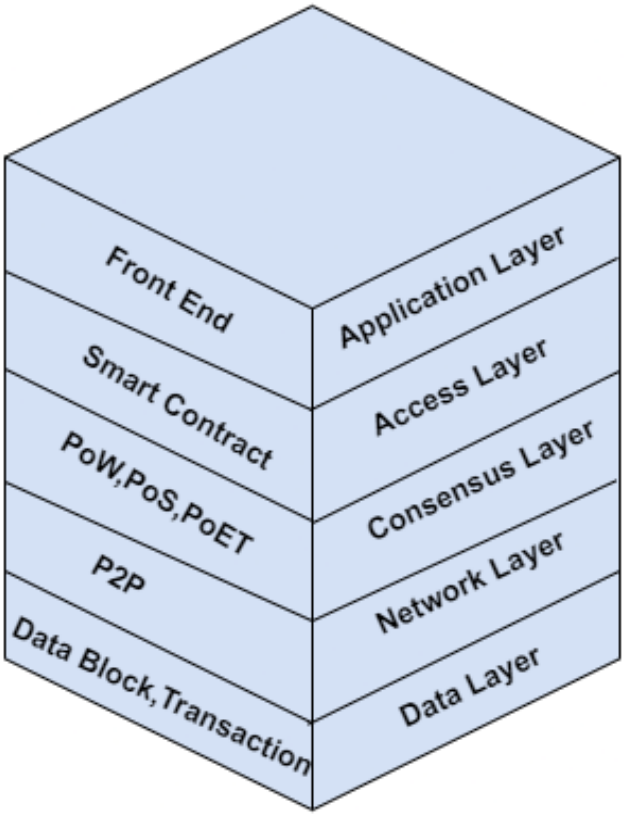

Figure 2. The layered architecture of blockchain-supported applications.

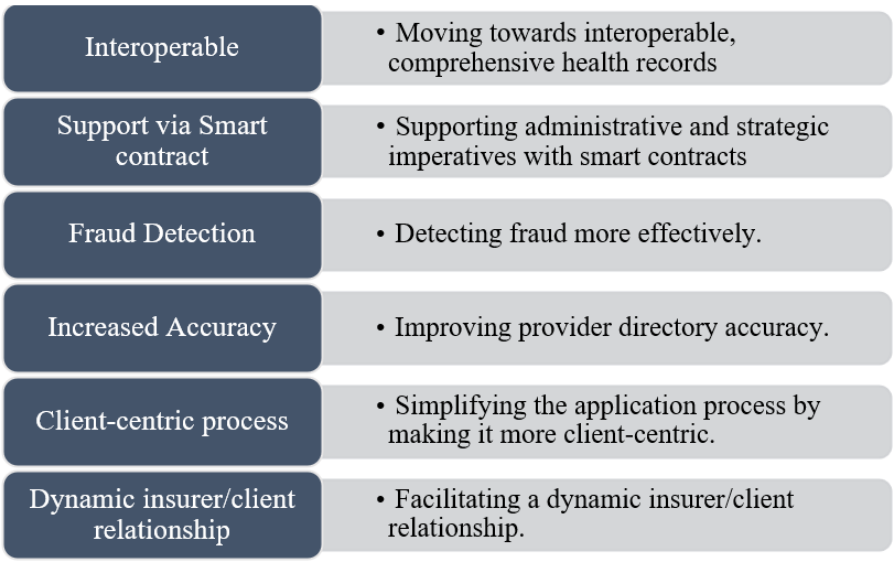

Figure 3. Benefits of employing blockchain technology in the healthcare industry.

4. Proposed Architecture

In our proposed architecture, a smart contract is created that provides metadata about record data, ownership, and permissions. Cryptographically signed instructions for controlling these characteristics are included in our system's blockchain transactions [50–53]. Only legal transactions ensuring data alternation are used by the contract's state-transition functionalities to carry out the rules. If a medical record can be represented computationally, laws may be built to enforce any set of rules governing it. For example, before providing third-party viewing access, a policy may require separate consent transactions from patients and healthcare providers. For complicated healthcare workflows, we created a solution based on blockchain smart contracts. Smart contracts are created to manage data access permissions across different actors in the healthcare ecosystem, as shown in Figure 4.

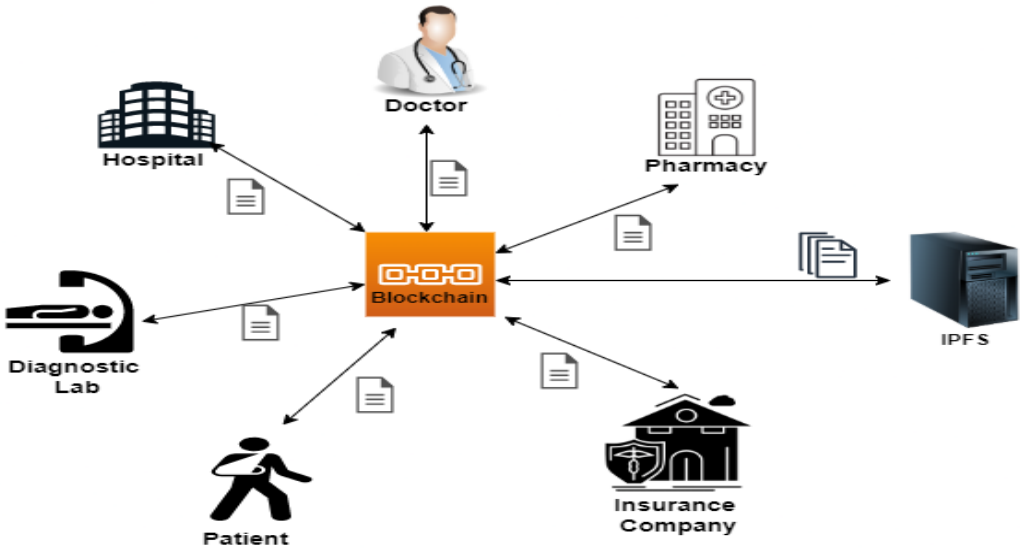

Figure 4. Blockchain and IPFS-supported healthcare ecosystems.

This will make it easier for all stakeholders to exchange and communicate information. Smart contracts include data authorization restrictions. It can also assist in tracing all actions associated with a unique ID from the point of origin to the current instance of time. There will be no need for a centralized organization to supervise and authorize the operation because this can be done directly through the smart contract, considerably

lowering the cost of administration. To ensure performance and economic sustainability, all medical record data are saved in interplanetary file storage, and the content identifier (CID) of the record is committed to the chain. The smart contract includes the registration of the entities, uploaded documents, treatment process details, and insurance claim process. The tools used in the implementation of the proposed work are shown in the Figure 5. It includes Solidity for smart contract development. It uses Truffle suit for the local blockchain environment. It employs web3.js library to connect the smart contract with the front end. Metamask wallet is used to enable the interaction of the code with the blockchain.

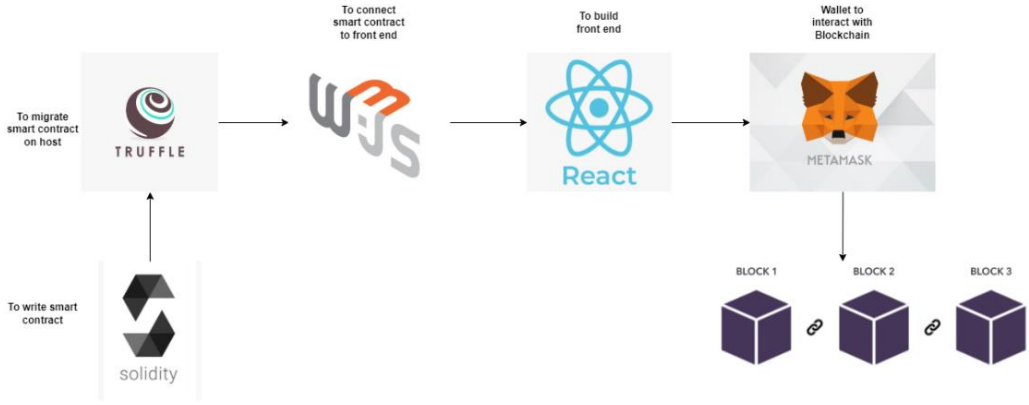

Figure 5. Different tools in the process flow.

5. Proposed Methodology

Multiple entities, such as patients, doctors, and insurance companies, are associated with the smart contract with the help of different functions, as shown in Figure 6. These entities interact with each other via smart contract functions.

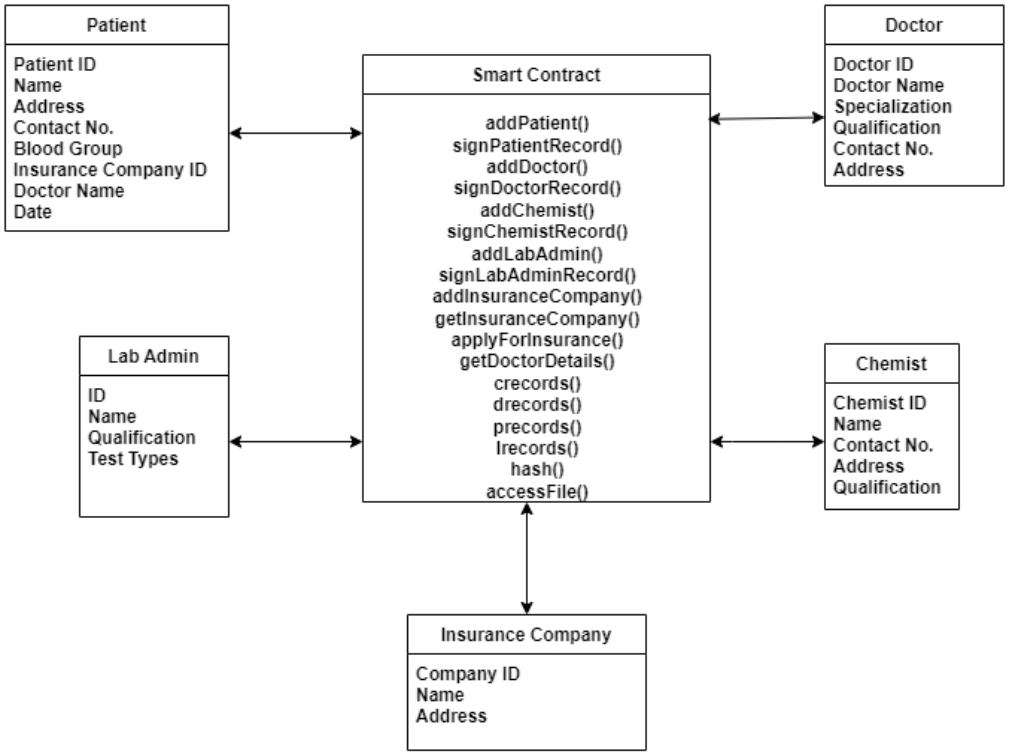

Figure 6. Entities associated with the smart contract.

The workflow of the process of record creation and insurance claim validation is shown in Figure 7. The proof-of-authority consensus procedure is employed in our suggested paradigm. Few selected nodes can function as validators in this algorithm to validate transactions. Because only preselected validator nodes will validate the transaction, the time necessary to create a block is predictable and smaller than the time required to generate a block using the PoW.

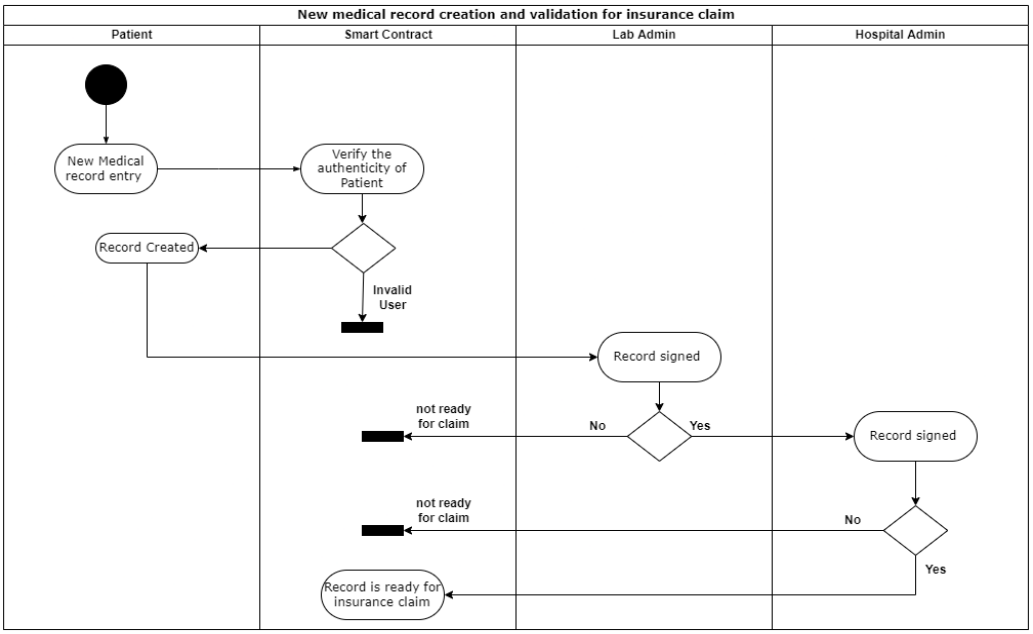

Figure 7. Workflow process.

5.1. Registration

The main entities in the proposed model are the hospital admin, patient, doctor, chemist, lab admin, and insurance company. The hospital admin add or register an entity by providing some information such as patient ID, name, address, etc. Then this record is signed and verified by the respective entity. An entity can sign and verify its respective record. One entity cannot sign and verify records of other entities' registration details. The address provided during registration is a 20-byte (160 bits or 40 hex characters) account address that will uniquely identify the entity in this model. All the entities are registered with a unique account address for the authentication purposes. Whenever any entity wants to access, verify, or update some information, then its hexadecimal address is used to authenticate the entity to check whether it is authorized to do so or not.

5.2. Treatment

At the time of treatment of any patient, information such as patient ID, doctor ID, diagnosis, test conducted, medicine, etc., are entered. This information can be retrieved at any point of time to find which doctor treated which patient, what type of tests were conducted, which medicine suggested, etc. Once the information is recorded in the blockchain transaction, nobody can update it after that. Even the doctor is not able to edit this information.

5.3. Document Upload on IPFS and Association with the Owner

Documents such as test reports, etc., are uploaded on IPFS. When a document is uploaded on IPFS, a content identifier (CID) is returned which is unique for each document. If there is any change in the content of the document, then its CID will also be changed. Two identical documents will generate the same CID. This CID is associated with a hexadecimal address. So, that entity with the associated address is treated as the owner of the document.

5.4. Insurance Claim

First, patients will create a medical record by providing a few details such as ID, test name, date, hospital name, price etc. Then, this record will be signed by the hospital admin and lab admin of that hospital. After getting signed by both, the record is considered approved. Then this record will go through the insurance claim process (Algorithms 1 and 2).

Algorithm 1: Add New Entity

1. If (msg.sender $\neq$ $admin_{hospital}$)
2. Then "cannot add new entity E and operation declined"
3. Else "enter attributes for E to create a record"
4. If (E Signed (E_{record}))
5. Then "E_{record} approved"
6. Else "E_{record} is not approved"
7. If (X Signed(E_{record})) //X represents any other entity
8. Then "operation declined"

Algorithm 2: Approval of New Medical Record for Insurance Claim

1. Patient P try to create a medical record M_{record}
2. If ($P_{address}$ $\neq$ $Auth_{address}$)
3. Then "M_{record} rejected"
4. Else "M_{record} created"
5. If ($P_{address}$ Signed (M_{record}))
6. Then "operation declined"
7. If ($A_{hospital}$ signed ($A_{hospital}$ Signed (M_{record})) || A_{lab} Signed (A_{lab} Signed (M_{record})))
8. Then "operation declined"
9. If ($A_{hospital}$ Signed (M_{record}) && A_{lab} Signed (M_{record}))
10. Then "M_{record} approved for insurance claim"
11. Else "M_{record} not approved for insurance claim"

6. Result and Analysis

We deploy a smart contract using Remix IDE and a Metamask wallet, then a confirmation pops up from the Metamask wallet as shown in Figure 8. It shows the activity of the transaction confirmation before its execution. Metamask wallet is used by the entities to connect with the system. This wallet stores the information about the account of the entities such as the number of ethers, address of the entity, etc.

This pop up shows the estimated gas fee required to deploy this smart contract. After clicking the confirm button, the smart contract is deployed, and the transaction is recorded in the distributed ledger of the blockchain. The transaction details show the address from which it is deployed, gas consumed, gas fee, etc., as shown in the Figure 9. These details include the status of the transaction, such as whether it is executed successfully or not. Transaction hash represents the hash of the executed transaction. From represents the address of the sender of the transaction. Gas represents the total gas available. Transaction cost represents the amount of gas consumed by this particular transaction.

After deployment, we can see a view of the different functions of the smart contract, as shown in Figure 10. Functions are shown with two different colors. Functions with orange color are those which will add or modify the state of the data. Functions with blue colour are only view functions. These functions do not change any data.

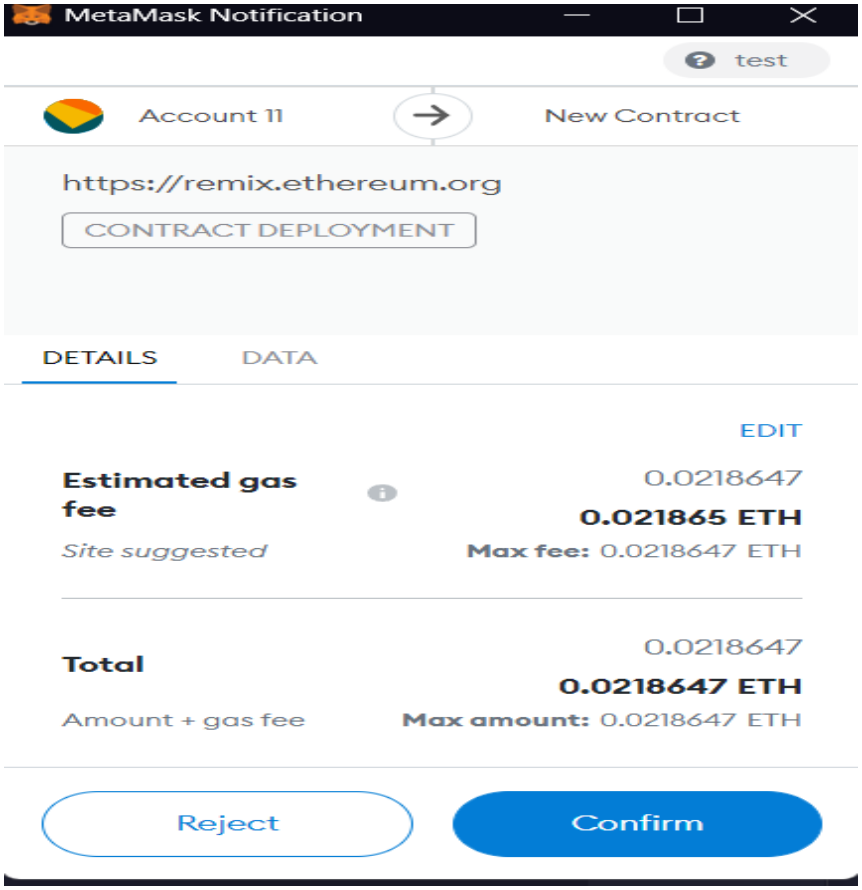

Figure 8. Smart contract deployment verification with Metamask.

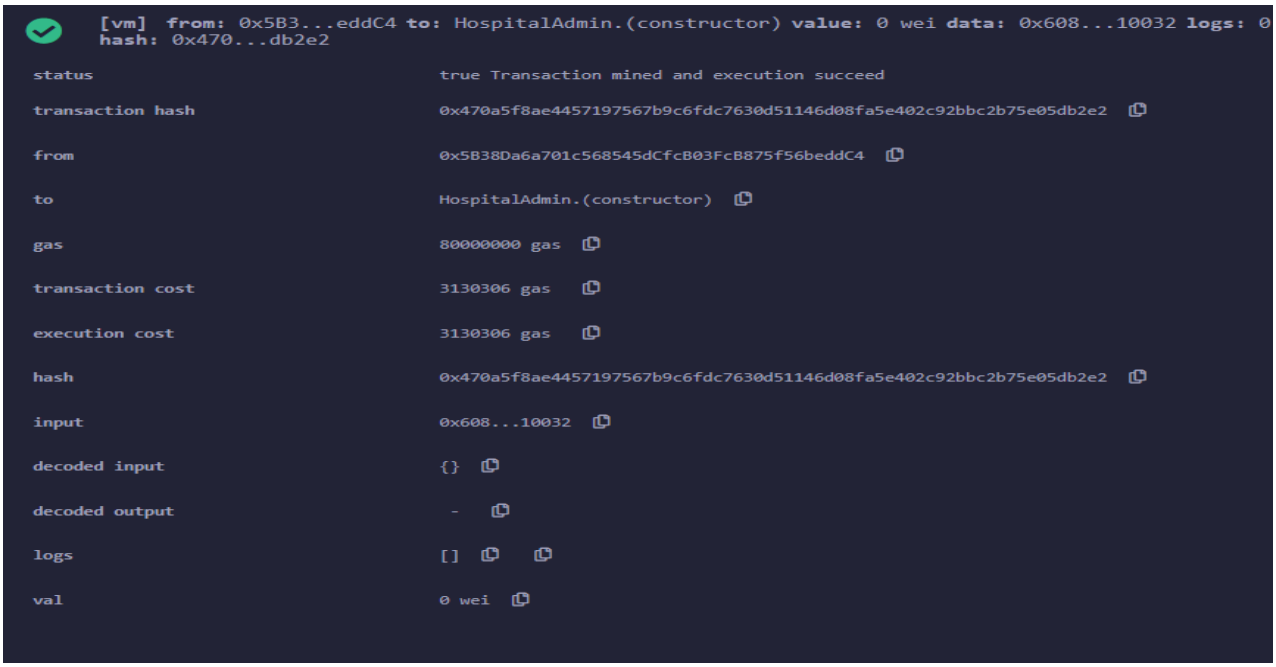

Figure 9. Smart contract deployment transaction details.

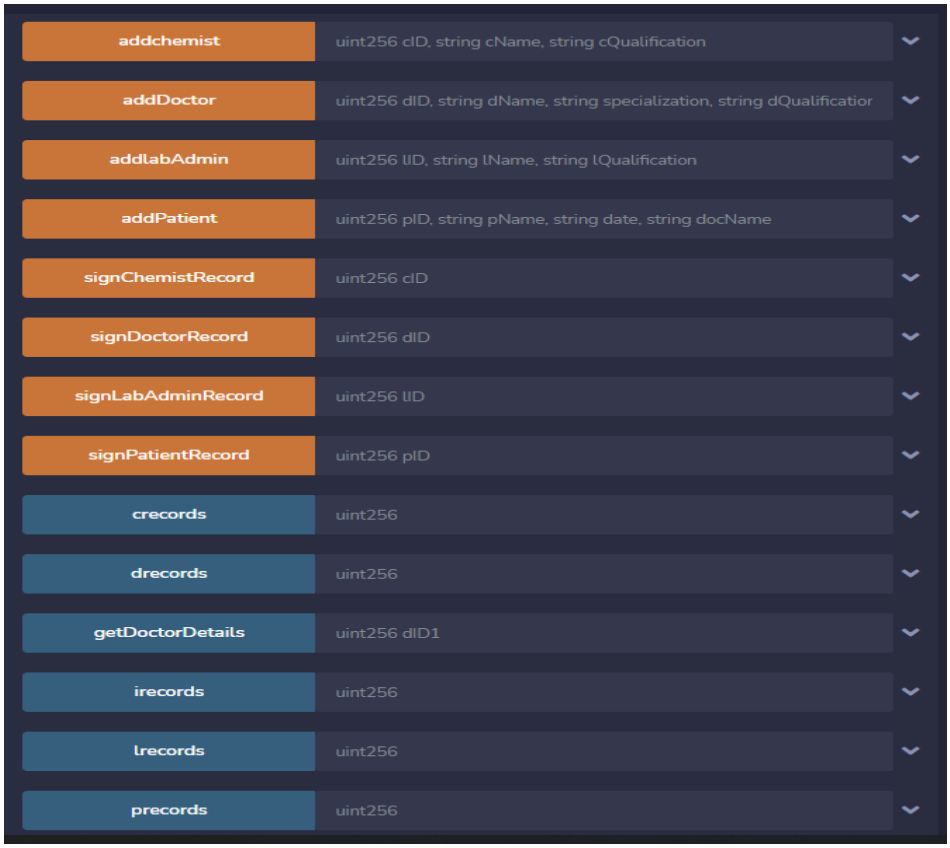

Figure 10. View after smart contract deployment.

After clicking on the addPatient function, a patient can be registered by the hospital admin as shown in Figure 11. For testing purposes, a patient with pID 11 named ram is registered. This patient is assigned to Dr. Shyam as per testing data.

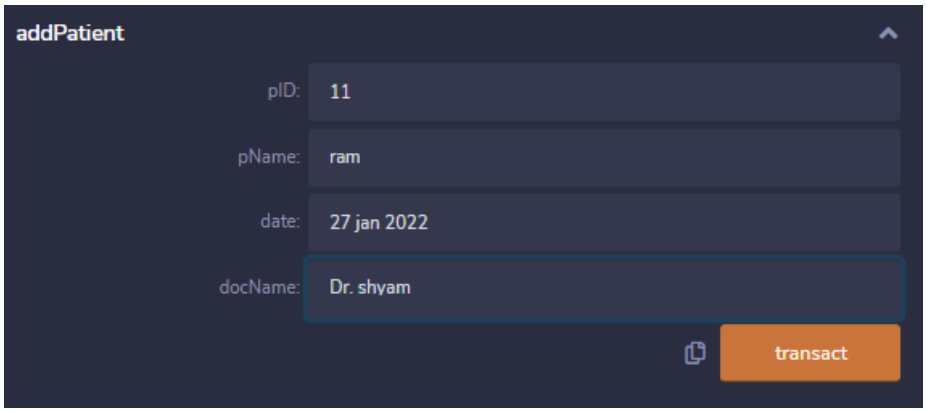

Figure 11. addPatient function of the smart contract.

After successful execution of the addPatient function, information related to this transaction such as the transaction hash, address by which this function is executed, gas available for execution, gas consumption by the function execution, and other related data can be seen in its transaction details, as shown in Figure 12.

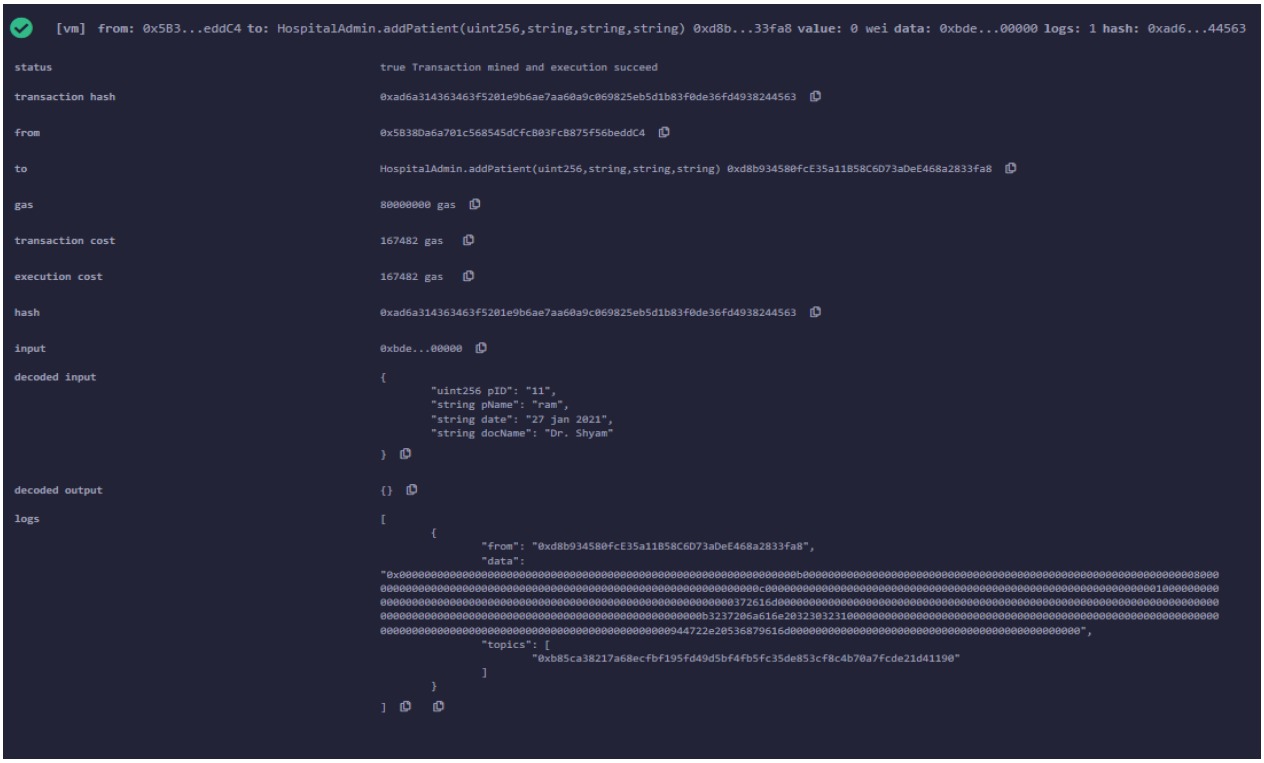

Figure 12. Transaction details of addPatient function execution.

If a hospital admin or any other entity tries to sign the record of a patient for verification, then the operation is declined. For example, if the address of the patient is "0xAb8 . . . 35cb2", but an entity with the address "0x5B3 . . . eddC4" tried to execute the function, then an error will be returned because only the patient with address "0xAb8 . . . 35cb2" can execute this function, as shown in Figures 13–15.

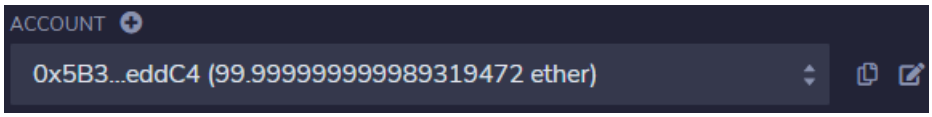

Figure 13. Account address of hospital admin.

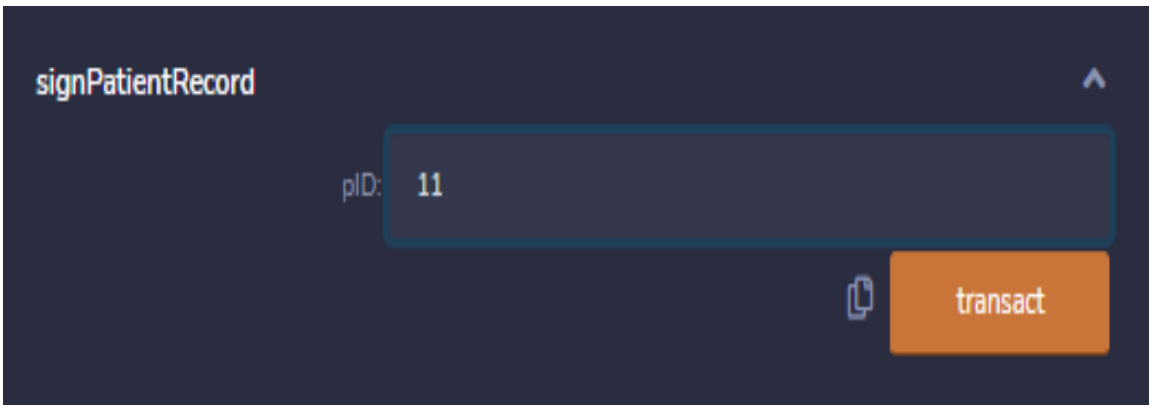

Figure 14. signPatientRecord function of the smart contract.

Figure 15. Patient record sign operation declined.

When the same function is used by the patient with address ""0xAb8 . . . 35cb2", then the function is executed and the transaction details for the same is recorded in the blockchain, as shown in Figures 16 and 17.

Figure 16. Patient account address.

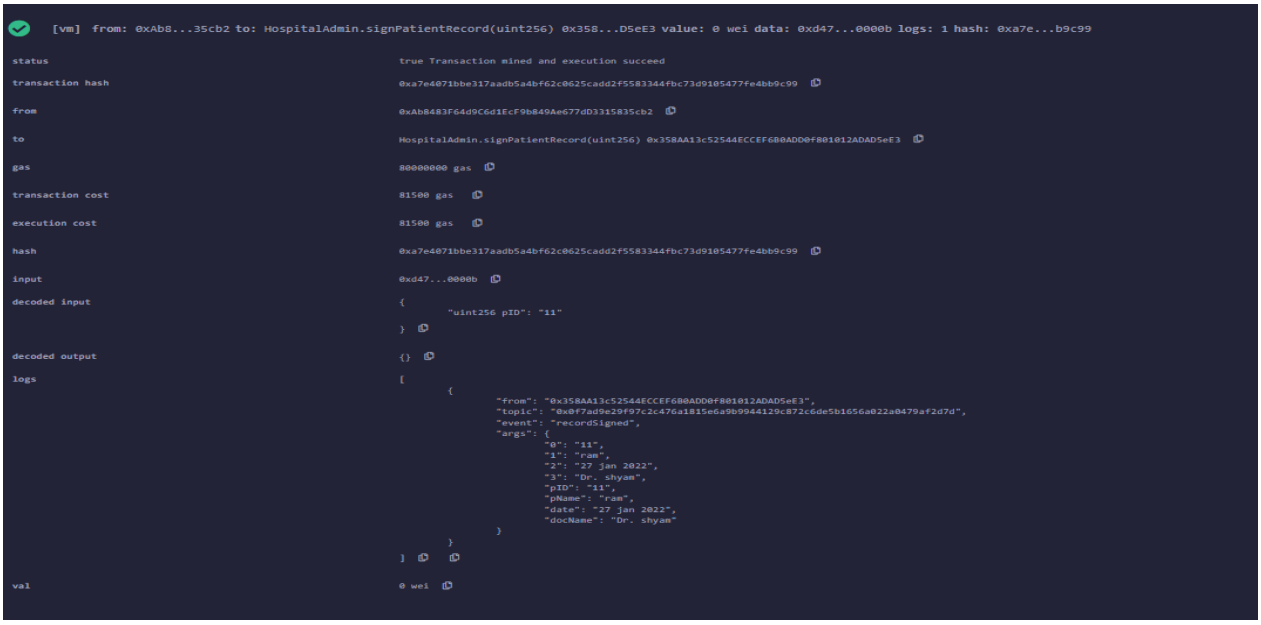

Figure 17. Transaction details of signPatientRecord function.

Medical documents such as test reports, etc., can be stored on IPFS, which is a decentralized storage solution. When a file is stored on IPFS, a content identifier (CID) is generated for that particular file. If there is any change in the file, then the CID will also be changed. For our implementation, a demo file is uploaded on IPFS, as shown in Figure 18.

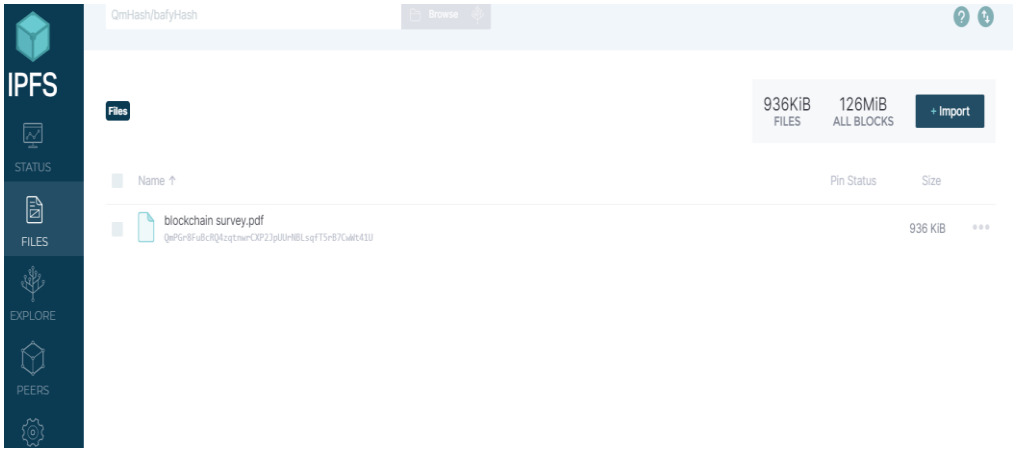

Figure 18. Demo file upload on IPFS.

After uploading the document, we can associate the CID of the document with the address of the owner of the file, as shown in Figure 19. For testing purposes, the CID used is "QmPGr8FuBcRQ4zqtnwrCXP2JpUUrNBLsqfT5rB7CwWt41U", and the owner address used is "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2".

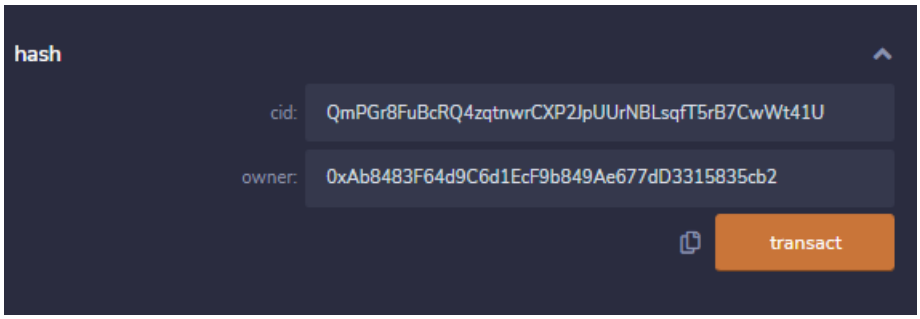

Figure 19. Function to bind ownership of IPFS file.

After successful execution of the hash function, information related to this transaction such as the transaction hash, address by which this function is executed, gas available for execution, gas consumption by the function execution, and other related data can be seen in the transaction details, as shown in Figure 20.

If any other unauthorized entity tries to access this file with CID "QmPGr8FuBcRQ4zqtnwrCXP2JpUUrNBLsqfT5rB7CwWt41U", then that operation is declined, as shown in Figures 21 and 22.

However, if the owner of the file with address "0xAb8483F64d9-C6d1EcF9b849Ae677dD3315835cb2" tries to access the same file, then this operation is allowed and the transaction is recorded in the blockchain, as shown in Figure 23.

When a smart contract is deployed on the main net of the Ethereum blockchain, it uses some fee for its deployment. This fee is necessary to avoid fake executions and keep the network running without intervention from an external entity. This fee is measured in terms of gas consumed for the execution. How much computation is required for execution of a transaction is represented by gas. The gas fee is paid in the local currency of the Ethereum blockchain, i.e., ether. The total amount of gas consumed for the execution of any transaction is multiplied with the gas price at that moment. This gives us the number of ethers required for the execution of that transaction. Then, the number of ethers can be multiplied with the USD price of ether to find the cost in USD. The gas price is different for different execution speeds. There are three types of executions: fast, standard, and slow. Miners receive some reward from the transaction fees of all the transactions included in the generated block. So, the Miners prioritize the transaction according to their gas fee. It

means a transaction with a high gas price is added in the block before a transaction with a low gas price. So, gas price is highest for fast executions and at its minimum for slow executions. Cost estimates for fast, standard, and slow executions for different functions of the smart contract are shown in Tables 1–3. The cost in ether and USD is calculated for different functions of the smart contract. If the user does not have a sufficient amount of gas in their wallet, then they cannot perform the transaction. The ether price in USD and the gas price for fast, standard, and slow executions are considered at the time of deployment of the contract.

Figure 20. Transaction details for ownership function.

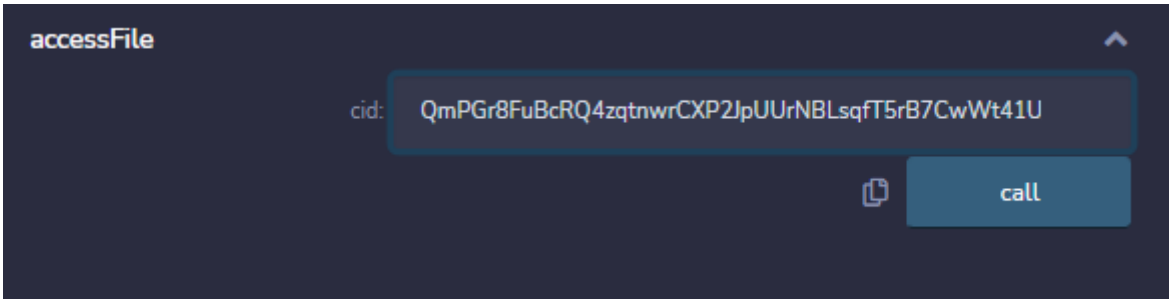

Figure 21. accessFile function of the smart contract.

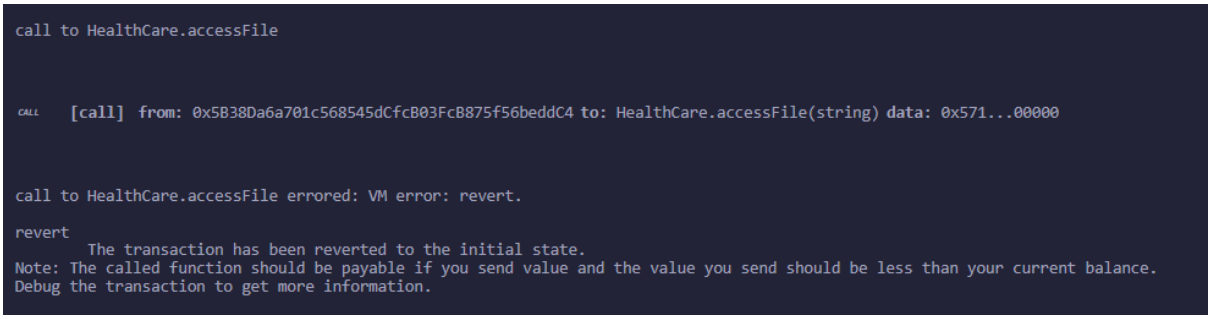

Figure 22. accessFile operation declined.

Figure 23. Transaction details for the accessFile function.

Table 1. Cost estimate for fast executions of transactions.

Gas Price in ETH = 0.000000122, ETH Price (USD) = 2740				
Sr.No.	**Function**	**Gas Consumed (GWEI)**	**Cost for Fast Execution (ETH)**	**Cost for Fast Execution (USD)**
1	addPatient	167,933	0.020487826	56.13664324
2	addDoctor	167,368	0.020418896	55.94777504
3	addChemist	143,061	0.017453442	47.82243108
4	addlabAdmin	143,023	0.017448806	47.80972844
5	signPatientRecord	81,699	0.009967278	27.31034172
6	signDcoctorRecord	83,693	0.010210546	27.97689604
7	signChemistRecord	80,596	0.009832712	26.94163088
8	signLabAdmin	80,332	0.009800504	26.85338096
9	getDoctorDetails	32,941	0.004018802	11.01151748

Table 1. *Cont.*

Gas Price in ETH = 0.000000122, ETH Price (USD) = 2740				
10	precord	39,277	0.004791794	13.12951556
11	hash	45,872	0.005596384	15.33409216
12	accessFile	25,434	0.003102948	8.50207752

Table 2. Cost estimate for standard executions of transactions.

Gas Price in ETH = 0.000000115, ETH Price (USD) = 2740				
Sr.No.	**Function**	**Gas Consumed (GWEI)**	**Cost for Standard Execution (ETH)**	**Cost for Standard Execution (USD)**
1	addPatient	167,933	0.019312295	52.9156883
2	addDoctor	167,368	0.01924732	52.7376568
3	addChemist	143,061	0.016452015	45.0785211
4	addlabAdmin	143,023	0.016447645	45.0665473
5	signPatientRecord	81,699	0.009395385	25.7433549
6	signDcoctorRecord	83,693	0.009624695	26.3716643
7	signChemistRecord	80,596	0.00926854	25.3957996
8	signLabAdmin	80,332	0.00923818	25.3126132
9	getDoctorDetails	32,941	0.003788215	10.3797091
10	precord	39,277	0.004516855	12.3761827
11	hash	45,872	0.00527528	14.4542672
12	accessFile	25,434	0.00292491	8.0142534

Table 3. Cost estimate for slow executions of transactions.

Gas Price in ETH = 0.000000109, ETH Price (USD) = 2740				
Sr.No.	**Function**	**Gas Consumed (GWEI)**	**Cost for Slow Execution (ETH)**	**Cost for Slow Execution (USD)**
1	addPatient	167,933	0.018304697	50.15486978
2	addDoctor	167,368	0.018243112	49.98612688
3	addChemist	143,061	0.015593649	42.72659826
4	addlabAdmin	143,023	0.015589507	42.71524918
5	signPatientRecord	81,699	0.008905191	24.40022334
6	signDcoctorRecord	83,693	0.009122537	24.99575138
7	signChemistRecord	80,596	0.008784964	24.07080136
8	signLabAdmin	80,332	0.008756188	23.99195512
9	getDoctorDetails	32,941	0.003590569	9.83815906
10	precord	39,277	0.004281193	11.73046882
11	hash	45,872	0.005000048	13.70013152
12	accessFile	25,434	0.002772306	7.59611844

A cost comparison of fast, standard, and slow executions of the transactions is shown in Figure 24.

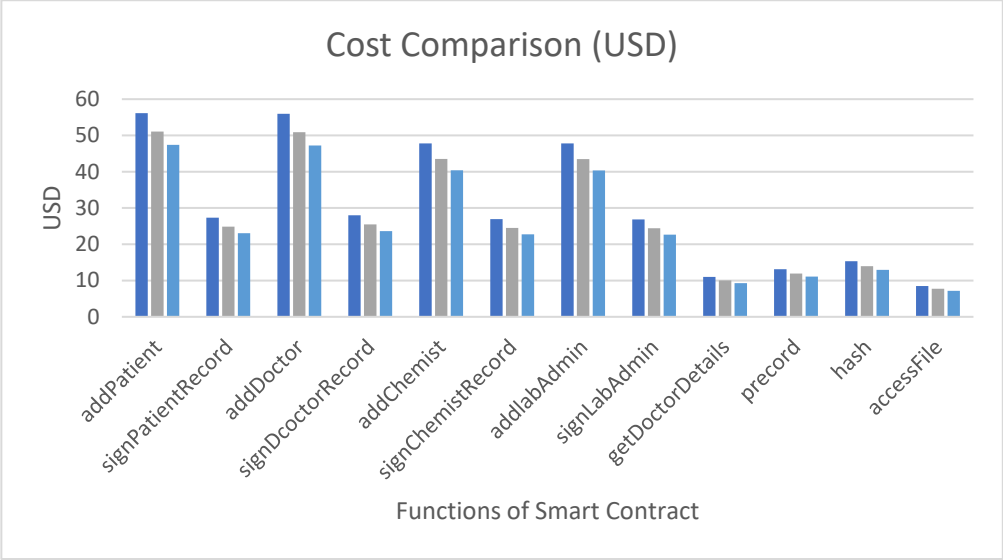

Figure 24. Cost comparison of fast, standard and slow execution of transactions.

The Ethereum blockchain is used for the deployment of the proposed solution. Use of the Ethereum blockchain is increasing day by day. More and more addresses are being registered on it, as shown in Figure 25. The gas price on the Etherum blockchain change daily. The average gas price during 2016 to 2022 is shown in Figure 26. As the number of registered users are increasing, the daily transaction execution count is also increasing, as shown in Figure 27.

Figure 25. Growth in active addresses on Ethereum (source: etherscan.io).

Existing approaches are compared with the proposed approach on the basis of various attributes. These attributes include the speed of transaction executions, energy consumption, processing power requirements, consensus algorithm, possibility of 51% attack, etc. Comparative analysis of the proposed approach with the existing approach is shown in Table 4. Existing approaches [15,42] use proof of work as the consensus algorithm. In this algorithm, a transaction is confirmed when multiple miners validate that particular transaction. Limitations with this process are its consumption of lots of energy, slow confirmation, and problem of 51% attack. In the proposed approach, the proof-of-authority consensus algorithm is used. In this process, predefined, limited nodes have the capability to validate the transactions. Energy consumption is low and confirmation of transactions is fast.

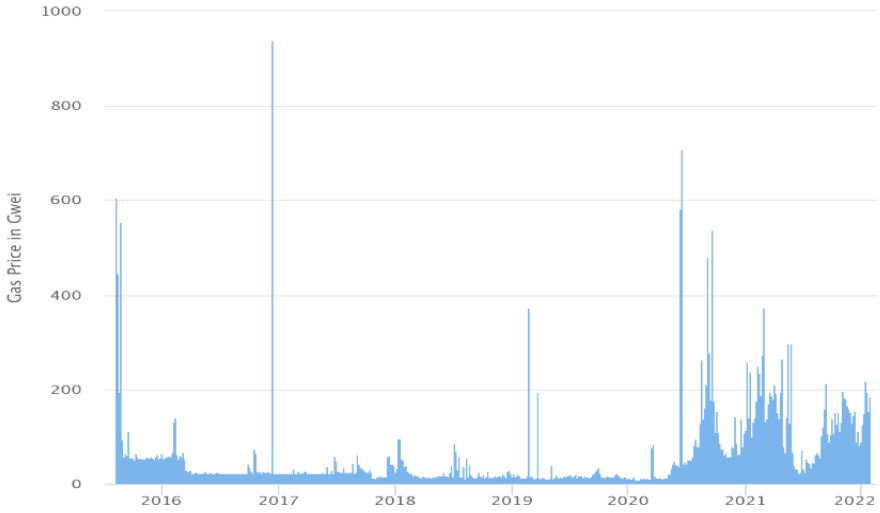

Figure 26. Average gas price on the Ethereum blockchain (source: etherscan.io).

Figure 27. Growth in daily transactions on the Ethereum blockchain (source: etherscan.io).

Table 4. Comparative analysis of the proposed approach with the existing approach.

Attributes	Proposed Approach	Existing Approache [15,42]
Transaction execution	Fast	Slow
Chances of 51% attack	Low	High
Energy Consumption	Low	High
Processing power requirement	Low	High
Validators	Fixed	Public
Consensus	PoA	PoW
Scalability	High	Low

7. Research Implications

In this study, we used blockchain technology to increase healthcare system interoperability across various stakeholders. Academicians, researchers, etc., can take benefit from our findings in a variety of ways. First and foremost, the findings may be used to improve policy formulation. Second, this research may be utilized as a foundation for looking into other parts of the healthcare sector where blockchain technology could be employed. The

findings provide a comprehensive perspective on a blockchain-enabled healthcare system. Researchers will be able to better comprehend the evolution and current state of blockchain technology, which will aid in the selection of worthwhile study areas that require more attention from the academic community. For cost-effective and secure data sharing, more blockchain-based apps may be developed.

8. Conclusions

In traditional healthcare delivery models, hospitals, laboratories, payers (i.e., insurance companies), and medication firms all store medical data related to patients in different forms, but have no consistency in record keeping. This has resulted in the current state of data chaos in the interchange of health records. We present a novel method for medical record management that uses smart contracts to provide auditability, interoperability, and accessibility. This system, which is planned to record flexibility and granularity, allows for the exchange of patients' medical data as well as insurance claims to support the system.

The practical application of distributed ledger technology in the medical domain will benefit many people, including health experts, healthcare workers, healthcare entities, and biomedical researchers, by allowing them to more effectively disseminate large amounts of data, share clinical knowledge, and communicate recommendations, while maintaining greater security and privacy protection. The effective deployment of this technology in medical settings in the healthcare domain will undoubtedly open new research paths for biomedical research development. Deployment of the proposed solution on other blockchains with lower costs can be considered as a future work. The lack of competence is a major barrier to the use of this modern technology in medical institutions. Blockchain applications are still in their infancy, and more effort in research is required. It does, however, serve as a responsibility of medical groups and regulators. The use of blockchain in healthcare is extremely likely to grow in the future. Its applications in healthcare will improve as a result of this technological advancement, since it aids in the explanation of treatment results and progress.

Author Contributions: Contributions: Conceptualization, S.K.R. (Sumit Kumar Rana), S.K.R. (Sanjeev Kumar Rana); methodology, S.K.R. (Sumit Kumar Rana), K.N., A.A.A.I., S.K.R. (Sanjeev Kumar Rana); validation, P.C., A.K.R., K.N., S.K.R. (Sanjeev Kumar Rana); formal analysis, S.K.R. (Sumit Kumar Rana), A.K.R., K.N., A.A.A.I., S.K.R. (Sanjeev Kumar Rana); data curation, S.K.R. (Sumit Kumar Rana), A.K.R., K.N., A.A.A.I., S.K.R. (Sanjeev Kumar Rana); writing—original draft preparation, N.G., K.N., A.A.A.I., S.K.R. (Sanjeev Kumar Rana); writing—review and editing, S.K.R. (Sumit Kumar Rana), A.K.R., and K.N.; supervision, K.N. and A.A.A.I.; project administration, K.N., and A.A.A.I.; funding acquisition, K.N. and A.A.A.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research work is fully supported by Faculty of Computing and Informatics University, Malaysia Sabah Jalan UMS, Kota Kinabalu Sabah 88400, Malaysia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
2. Hyla, T.; Peja´s, J. Long-term verification of signatures based on a blockchain. *Comput. Electr. Eng.* **2020**, *81*, 106523. [CrossRef]
3. Kumar, G.; Saha, R.; Rai, M.K.; Thomas, R.; Kim, T.H. Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics. *IEEE Internet Cings J.* **2019**, *6*, 6835–6842. [CrossRef]
4. Thomason, J.; Ahmad, M.; Bronder, P.; Hoyt, E.; Pocock, S.; Bouteloupe, J.; Donaghy, K.; Huysman, D.; Willenberg, T.; Joakim, B.; et al. Blockchain—Powering and empowering the poor in developing countries. In *Transforming Climate Finance and Green Investment with Blockchains*; Academic Press: Cambridge, MA, USA, 2018.

5. Clauson, K.A.; Breeden, E.A.; Davidson, C.; Mackey, T.K. Leveraging blockchain technology to enhance supply chain management in healthcare: An exploration of challenges and opportunities in the health supply chain. *Blockchain Healthc. Today* **2018**, *1*, 1–12. [CrossRef]
6. Sylim, P.; Liu, F.; Marcelo, A.; Fontelo, P. Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention. *JMIR Res. Protoc.* **2018**, *7*, e10163. [CrossRef]
7. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [CrossRef]
8. Hathaliya, J.J.; Tanwar, S.; Tyagi, S.; Kumar, N. Securing electronics healthcare records in healthcare 4.0: A biometricbased approach. *Comput. Electr. Eng.* **2019**, *76*, 398–410. [CrossRef]
9. Azzi, R.; Chamoun, R.K.; Sokhn, M. The power of a blockchain-based supply chain. *Comput. Ind. Eng.* **2019**, *135*, 582–592. [CrossRef]
10. Bhutta, M.N.M.; Bhattia, S.; Alojail, M.A.; Nisar, K.; Cao, Y.; Chaudhry, S.A.; Sun, Z. Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS). *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 10. [CrossRef]
11. Kumar, A.; Sharma, S.; Singh, A.; Alwadain, A.; Choi, B.J.; Manual-Brenosa, J.; Goyal, N. Revolutionary Strategies Analysis and Proposed System for Future Infrastructure in Internet of Things. *Sustainability* **2021**, *14*, 71. [CrossRef]
12. Francisco, K.; Swanson, D. The Supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics* **2018**, *2*, 2. [CrossRef]
13. Verhoeven, P.; Sinn, F.; Herden, T. Examples from blockchain implementations in logistics and supply chain management: Exploring the mindful use of a new technology. *Logistics* **2018**, *2*, 20. [CrossRef]
14. Figorilli, S.; Antonucci, F.; Costa, C. A Blockchain Implementation Prototype for the Electronic Open Source Traceability of Wood along the Whole Supply Chain. *Sensors* **2018**, *18*, 3133. [CrossRef] [PubMed]
15. Lemieux, V.L. Trusting records: Is Blockchain technology the answer? *Rec. Manag. J.* **2016**, *26*, 110–139. [CrossRef]
16. Weber, I.; Xu, X.; Riveret, R.; Governatori, G.; Ponomarev, A.; Mendling, J. Untrusted business process monitoring and execution using blockchain. In Proceedings of the International Conference on Business Process Management, Rome, Italy, 6–10 September 2016; Springer: Cham, Switzerland, 2016.
17. Waseem, Q.; Alshamrani, S.S.; Nisar, K.; Wan Din, W.I.S.; Alghamdi, A.S. Future Technology: Software-Defined Network (SDN) Forensic. *Symmetry* **2021**, *13*, 767. [CrossRef]
18. Daisuke, I.; Kashiyama, M.; Ueno, T. Tamper-resistant mobile health using blockchain technology. *JMIR Mhealth Uhealth* **2017**, *5*, e111.
19. Vazirani, A.A.; O'Donoghue, O.; Brindley, D.; Meinert, E. Implementing Blockchains for Efficient Health Care: Systematic Review. *J. Med. Internet Res.* **2019**, *21*, e12439. [CrossRef]
20. Ahmad, Z.; Khan, A.S.; Nisar, K.; Haider, I.; Hassan, R.; Haque, M.; Tarmizi, S.; Rodrigues, J. Anomaly Detection Using Deep Neural Network for IoT Architecture. *Appl. Sci.* **2021**, *11*, 7050. [CrossRef]
21. Sabir, Z.; Ibrahim, A.A.A.; Raja, M.A.Z.; Nisar, K.; Umar, M.; Rodrigues, J.J.P.C.; Mahmoud, S.R. Soft Computing Paradigms to Find the Numerical Solutions of a Nonlinear Influenza Disease Model. *Appl. Sci.* **2021**, *11*, 8549. [CrossRef]
22. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient Healthcare Data Sharing via Blockchain. *Appl. Sci.* **2019**, *9*, 1207. [CrossRef]
23. Haque, M.R.; Tan, S.C.; Yusoff, Z.; Nisar, K.; Lee, C.K.; Kaspin, R.; Shankar Chowdhry, B.; Buyya, R.; Prasad Majumder, S.; Gupta, M.; et al. Automated controller placement for software-defined networks to resist DDoS attack. *Comput. Mater. Contin.* **2021**, *68*, 3147–3165. [CrossRef]
24. Litchfield, A.T.; Khan, A. A Review of Issues in Healthcare Information Management Systems and Blockchain Solutions. In Proceedings of the CONF-IRM, International Conference on Information Resources Management, CONF-IRM 2019, Auckland, New Zealand, 27–29 May 2019.
25. Wei, L.L.Y.; Ibrahim, A.A.A.; Nisar, K.; Ismail, Z.I.A.; Welch, I. Survey on Geographic Visual Display Techniques in Epidemiology: Taxonomy and Characterization. *J. Ind. Inf. Integr.* **2020**, *18*, 1–14. [CrossRef]
26. Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G. Blockchain Technology Use Cases in Healthcare. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2018; Volume 111, pp. 1–41.
27. Sodhro, A.H.; Al-Rakhami, M.S.; Wang, L.; Magsi, H.; Zahid, N.; Pirbhulal, S.; Nisar, K.; Ahmad, A. Decentralized Energy Efficient Model for Data Transmission in IoT-based Healthcare System. In Proceedings of the 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), Helsinki, Finland, 25–28 April 2021; pp. 1–5. [CrossRef]
28. Shuja, J.; Ahmad, R.W.; Gani, A.; Ahmed, A.I.A.; Siddiqa, A.; Nisar, K.; Khan, S.U.; Zomaya, A.Y. Greening emerging IT technologies: Techniques and practices. *J. Internet Serv. Appl. (JISA)* **2017**, *89*, 1–11. [CrossRef]
29. Lee, S.H.; Yang, C.S. Fingernail analysis management system using microscopy sensor and blockchain technology. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 1550147718767044. [CrossRef]
30. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain technology in healthcare: A systematic review. *Healthcare* **2019**, *7*, 56. [CrossRef]
31. Haider, I.; Khan, K.B.; Haider, M.A.; Saeed, A.; Nisar, K. Automated Robotic System for Assistance of Isolated Patients of Coronavirus (COVID-19). In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 5–7 November 2020; pp. 1–6. [CrossRef]

32. Haider, I.; Mehdi, M.A.; Amin, A.; Nisar, K. A Hand Gesture Recognition based Communication System for Mute people. In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 5–7 November 2020; pp. 1–6. [CrossRef]
33. Kumar, T.; Ramani, V.; Ahmad, I.; Braeken, A.; Harjula, E.; Ylianttila, M. Blockchain Utilization in Healthcare: Key Requirements and Challenges. In Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, Czech Republic, 17–20 September 2018.
34. Genestier, P.; Zouarhi, S.; Limeux, P.; Excoer, D.; Prola, A.; Sandon, S.; Temerson, J.M. Blockchain for consent management in the ehealth environment: A nugget for privacy and security challenges. *J. Int. Soc. Telemed. Ehealth* **2017**, *5*, GKR-e24.
35. Chowdhry, B.S.; Shah, A.A.; Harris, N.; Hussain, T.; Nisar, K. Development of a Smart Instrumentation for Analyzing Railway Track Health Monitoring Using Forced Vibration. In Proceedings of the 2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT), Tashkent, Uzbekistan, 7–9 November 2020; pp. 1–5. [CrossRef]
36. Boulos, M.N.K.; Wilson, J.T.; Clauson, K.A. Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. *Int. J. Health Geogr.* **2018**, *17*, 25. [CrossRef]
37. Khatoon, A. A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics* **2020**, *9*, 94. [CrossRef]
38. Thomas, J. Medical records and issues in negligence. *Indian J. Urol.* **2009**, *25*, 384–388. [CrossRef]
39. Thenmozhi, M.; Dhanalakshmi, R.; Geetha, S.; Valli, R. Implementing blockchain technologies for health insurance claim processing in hospitals. In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 5–7 November 2020.
40. Pandit, M.; Gupta, D.; Anand, D.; Goyal, N.; Aljahdali, H.M.; Mansilla, A.O.; Kumar, A. Towards Design and Feasibility Analysis of DePaaS: AI Based Global Unified Software Defect Prediction Framework. *Appl. Sci.* **2022**, *12*, 493. [CrossRef]
41. Nisar, K.; Ibrahim, A.A.A.; Wu, L.; Adamov, A.; Deen, M.J. Smart home for elderly living using Wireless Sensor Networks and an Android application. In Proceedings of the 2016 10th IEEE International Conference on Application of Information and Communication Technologies AICT2016, Azerbaijan, Baku, 12–14 October 2016; pp. 1–8. [CrossRef]
42. Rana, S.K.; Rana, S.K. Blockchain based business model for digital assets management in trust less collaborative environment. *J. Crit. Rev.* **2020**, *7*, 738–750.
43. Lilhore, U.K.; Imoize, A.L.; Lee, C.-C.; Simaiya, S.; Pani, S.K.; Goyal, N.; Kumar, A.; Li, C.-T. Enhanced Convolutional Neural Network Model for Cassava Leaf Disease Identification and Classification. *Mathematics* **2022**, *10*, 580. [CrossRef]
44. Jamil, F.; Qayyum, F.; Alhelaly, S.; Javed, F.; Muthanna, A. Intelligent Microservice Based on Blockchain for Healthcare Applications. *Comput. Mater. Contin.* **2021**, *69*, 2513–2530. [CrossRef]
45. Kumar, A.; Sharma, S. IFTTT rely based a semantic web approach to simplifying trigger-action programming for end-user application with IoT applications. In *Semantic IoT: Theory and Applications*; Springer: Cham, Switzerland, 2021; pp. 385–397.
46. Khezr, S.; Moniruzzaman, M.; Yassine, A.; Benlamri, R. Blockchain technology in healthcare: A comprehensive review and directions for future research. *Appl. Sci.* **2019**, *9*, 1736. [CrossRef]
47. Rana, A.K.; Sharma, S. Industry 4.0 manufacturing based on IoT, cloud computing, and big data: Manufacturing purpose scenario. In *Advances in Communication and Computational Technology*; Springer: Singapore, 2021; pp. 1109–1119.
48. Ratta, P.; Kaur, A.; Sharma, S.; Shabaz, M.; Dhiman, G. Application of Blockchain and Internet of Things in Healthcare and medical sector: Application, challenges and future prespectives. *J. Food Qual.* **2021**, *2021*, 1–20. [CrossRef]
49. Rana, A.K.; Sharma, S. Enhanced energy-efficient heterogeneous routing protocols in WSNs for IoT application. *IJEAT* **2019**, *9*, 4418–4425. [CrossRef]
50. Hasselgren, A.; Rensaa, J.A.H.; Kralevska, K.; Gligoroski, D.; Faxvaag, A. Blockchain for Increased Trust in Virtual Health Care Proof-of-Concept Study. *J. Med. Internet Res.* **2021**, *23*, 1–15. [CrossRef]
51. Sarkar, N.I.; Kuang, A.X.M.; Nisar, K.; Amphawan, A. Performance Studies of Integrated Network Scenarios in a Hospital Environment. *Int. J. Inf. Commun. Technol. Hum. Dev. (IJICTHD)* **2014**, *6*, 35–68. [CrossRef]
52. Rana, A.K.; Sharma, S. Contiki Cooja Security Solution (CCSS) with IPv6 routing protocol for low-power and lossy networks (RPL) in Internet of Things applications. In *Mobile Radio Communications and 5G Networks*; Springer: Singapore, 2021; pp. 251–259.
53. Rana, S.K.; Kim, H.C.; Pani, S.K.; Rana, S.K.; Joo, M.I.; Rana, A.K.; Aich, S. Blockchain-Based Model to Improve the Performance of the Next-Generation Digital Supply Chain. *Sustainability* **2021**, *13*, 10008. [CrossRef]
54. Kumar, A.; Sharma, S.; Goyal, N.; Singh, A.; Cheng, X.; Singh, P. Secure and energy-efficient smart building architecture with emerging technology IoT. *Comput. Commun.* **2021**, *176*, 207–217. [CrossRef]
55. Nisar, N.; Hasbullah, H. The Effect of Panoramic View of a Digital Map on User Satisfaction. In Proceedings of the International Symposium on Information Technology 2008 (ITSim2008), KLCC, Kuala Lumpur, Malaysia, 26–28 August 2008; pp. 1–4. [CrossRef]
56. Hasbullah, H.; Nisar, K.; Said, A. The effect of echo on voice quality in VoIP network. In Proceedings of the International Association for Science and Technology Development (IASTED) Calgary, AB, Canada; Advances in Computer Science and Engineering (ACSE): Phuket, Thailand, 2009; pp. 95–100, ISBN 978-088986790-1.
57. Nisar, N.; Said, A.M.; Hasbullah, H. Enhanced Performance of IPv6 Packet Transmission over VoIP Network. In Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology, Beijing, China, 11 August 2009; pp. 500–504. [CrossRef]

58. Nisar, K.; Said, A.M.; Hasbullah, H. Enhanced performance of WLANs packet transmission over VoIP Network. In Proceedings of the 2010 IEEE 24th International Conference on Advanced Information Networking and Applications, Workshops, (AINA 2010), Perth, Australia, 20–23 April 2010; pp. 485–490. [CrossRef]
59. Jimson, E.R.; Nisar, K.; bin Ahmad Hijazi, M.H. Bandwidth Management using Software Defined Network and Comparison of the Throughput Performance with Traditional Network. In Proceedings of the International Conference on Computer and Drone Applications (ICONDA) 2017, Kuching, Malaysia, 9–11 November 2017; pp. 71–76. [CrossRef]
60. Nisar, K.; Lawal, I.A.; Abualsaud, K.; El-Fouly, T.M. A New WDM Application Response Time in WLAN Network and Fixed WiMAX using Distributed. In Proceedings of the 11th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA' 2014), Doha, Qatar, 10–13 November 2014; pp. 781–787. [CrossRef]
61. Nisar, K.; Said, A.M.; Hasbullah, H. Enhanced Performance of Packet Transmission Using System Model Over VoIP Network. In Proceedings of the International Symposium on Information Technology 2010 (ITSim 2010), KLCC, Kuala Lumpur, Malaysia, 15 June 2010; pp. 1005–1008. [CrossRef]
62. Sattar, F.; Hussain, M.; Nisar, K. A secure architecture for open source VoIP solutions. In Proceedings of the IEEE International Conference on Information and Communication Technologies (ICICT), Karachi, Pakistan, 23–24 July 2011; pp. 1–6.
63. Rana, A.; Chakraborty, C.; Sharma, S.; Dhawan, S.; Pani, S.K.; Ashraf, I. Internet of Medical Things-Based Secure and Energy-Efficient Framework for Health Care. *Big Data* **2021**, *10*, 18–33. [CrossRef] [PubMed]
64. Joshi, S.; Sharma, M.; Das, R.P.; Muduli, K.; Raut, R.; Narkhede, B.E.; Shee, H.; Misra, A. Assessing Effectiveness of Humanitarian Activities against COVID-19 Disruption: The Role of Blockchain-Enabled Digital Humanitarian Network. *Sustainability* **2022**, *14*, 1904. [CrossRef]
65. Swain, S.; Peter, O.; Adimuthu, R.; Muduli, K. Blockchain technology for limiting the impact of pandemic. In *Computational Modelling and Data Analysis in COVID-19 Research*; CRC Press: Boca Raton, FL, USA, 2021; pp. 165–186.