Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES) – An International Journal
ISSN: 2566-932X, Vol. 4, Issue 6, September 2020
Part of the Proceedings of the 1st All India Paper writing Competition on Emerging Research - PaCER 2020

A Blockchain-Based Secure and Sustainable Electronic Healthcare Record System

Niharika P Kumar
Associate Professor, Dept. of Computer Science and Engineering, BNM Institute of Technology, Bengaluru, India, niharikaresearch7@gmail.com

Shreyas B
B.E., Dept. of Computer Science and Engineering, BNM Institute of Technology, Bengaluru, India, shreyasb63@gmail.com

Srinidhi S P
B.E., Dept. of Computer Science and Engineering, BNM Institute of Technology, Bengaluru, India, srinidhisp29@gmail.com

Abstract: In today's world, Data is the new gold. Data holds an exorbitant value in a plethora of areas. The increase in demand for data is directly proportional to Data Privacy. Blockchain is one of those technologies which helps in data privacy and facilitates data integrity and confidentiality. The healthcare sector is in constant need of data security, privacy, confidentiality and decentralization in electronic medical records. The objective of this paper is primarily to implement blockchain technology for electronic medical records and secondarily to provide secure storage of these records and define access rules for the users of the proposed system.

Keywords: Blockchain; Metamask; Electronic Medical Records(EMR); FHIR; Smart-Contract; Solidity; Ethereum

I. INTRODUCTION

Data is an important aspect of technology. Over the past decade the world has witnessed the rise in demand for data related to technology and recently, observations of data being used extensively in the healthcare sector has been noted. Till recent times, archaic ways of storing and manipulating data was used in the healthcare sector. These methodologies were inefficient and insecure and were not decentralized. Clinical records long for advancement. Patients leave information dispersed across different purviews. Soon after this primitive period, there was a significant advancement in the healthcare sector which brought about the digitalization of a patient's medical records. These new advancements allowed different medical institutions to access a particular patient's medical records and to provide an effective diagnosis. This feature also gave the medical institutions insight into the treatment of different ailments and its cure which helped them in preparing beforehand if similar circumstances were to befall upon them. Even though these electronic medical records revolutionized patient data sharing, it also came along with a few vulnerabilities. Firstly, the data shared was not confidential and thus it allowed a third party to access the sensitive details of patients. Secondly, since the data was mutable, there was a significant scope in tampering and altering the patient's personal information. Thirdly, the deployment of the said system was tedious and needed trained personnel. These vulnerabilities compromised the data integrity and privacy of a patient.

There has been a steep rise in the number of patients due to the Covid-19 pandemic and as a consequence, there is a need for an efficient system to handle the medical records of all these patients, which would allow the said patient to authorize who can access his/her electronic medical records. This paper proposes a solution combating the said vulnerabilities by implementing blockchain technology. This system strives to achieve data integrity and confidentiality while being able to achieve a large scale deployment among medical institutions. The electronic medical records in our system are immutable and hence cannot be tampered by third parties. The patient can restrict access to his/her medical records to only the personnel involved in his/her diagnosis. This system is proposed not as the catholicon for medical record management, but as an onset into this space to demonstrate innovative Electronic Medical Record solutions with blockchain technology.

This paper is structured as follows, section II of this paper describes the research work carried out in the field of EHR management using Blockchain; section III summarizes the basics of blockchain technology and smart contract along with its features. Section IV explains the blueprint and framework of the system and section V elucidates the performance of this system.

II. RELATED WORK

Blockchain technology was introduced to the world by Satoshi Nakamoto. The rudimentary philosophy behind bitcoin was- moneyless transactions, i.e. digital transactions. Blockchain was "the wheel" of technology which transformed not only transactions and the monetary system but it brought about major changes in numerous fields, including the healthcare sector. A plethora of researchers have carried out research in this area, the fundamental idea behind these researches is to figure out whether blockchain as a base will be able to perform, enhance and even create a new healthcare system which

may make the current system obsolete. The researchers have also been able to conjure results from their implementations and have brought up their sets of advantages, loopholes and even the challenges faced while deploying their systems. FHIR also known as Fast Healthcare Interoperability Resources is one of the major platforms where the exchange of patient data and manipulation of data can be done between two or more medical institutes or healthcare agencies.

In [1], authors discuss the application of blockchain technology to remote data exchange. The system proposed in this paper exhibits the power of blockchain to promote efficient healthcare data exchange while simultaneously making sure that the security of original data sources is intact. This proposed system institutes a public-key cryptography to generate and maintain health identities.

A blockchain-based approach to sharing patient data is explored in [2]. The system provides access to API's with the motive of sharing Electronic Medical Records. This system relies on FHIR which is an upcoming standard that portrays data configuration along its constituents.

In [3], the authors throw light on how the new Health Level Seven (HL7) standard in close association with FHIR standard has the potential to attain interoperability in healthcare systems. The new FHIR is based on RESTful principles and also implements incremental and iterative approach.

The proposed system in [4] is a new, decentralized or distributed record management system to maneuver electronic medical records with the aid of blockchain technology. The paper exemplifies a novel perspective for steering medical records by providing features such as audit-ability, interoperability and accessibility. The paper exhibits how concepts of decentralization can be enacted to extensive data organization in an electronic medical record system.

In [5], the author proposes a healthcare information exchange system, built on blockchain technology which is basically to share healthcare data from different sources to various healthcare service providers. The paper uses the principles of two fairness-based transaction packing algorithms to implement the proposed system. High output or outturn along with low latency and average fairness can be brought into this system with the help of two fairness-based transaction packing algorithms.

The proposed implementation in [6] highlights Blockchain-based approach to Medical-Healthcare data storage and service. The proposed system's framework is a Merkle Tree-based structure. For safe storage of data and for sharing of said private data, the proposed system implements blockchain technology and cloud storage Technology.

In [7], the author focuses on the two main challenges in this system, firstly, the security of sensitive data present on the blockchain network. Secondly, implementation and deployment of the system to hospital systems. The proposed system seeks to utilize the Ethereum platform for smart contract operations along with the use of Docker containers and uses microservices for distributed architecture.

In [8], the implementation starts off with the web/cloud platforms layer, which stores Patient healthcare Details in their own local databases. The cloud intermediate layer is the second layer, which links multiple virtual machines that are utilized in order to assure that there is no failure due to a collapse in one of the systems, which can lead to a system-wide failure unlike a centralized mounting where one customized server hosts the intermediate layer architecture. The deployment of smart contracts which oversee the sharing of data and authorization comes under the final layer which is the Blockchain network.

In [9], the paper explains a blockchain-based, mobile controlled, system for private health data sharing and alliance. The paper then speaks about system evaluation where the system fosters a user oriented model for refining private health data and uses a blockchain network, which assures the data confidentiality and coherence.

The authors describe instances of the implementations of blockchain technology in the health industry to solve real-world problems in [10]. The paper provides important considerations for the future of this technology namely, the challenges and risks. The paper concludes by stating the immense potential blockchain technology possesses in the healthcare domain with many new applications and executions being uncovered and evolved.

III. PREREQUISITES

This section throws light on the prerequisites used to implement the proposed system. This highlights the software platform used to implement this system and also its advantages. Ethereum and Smart contracts are the most important for this implementation and are also discussed in the following system.

A. MetaMask

Metamask is a search engine extension which runs on Ethereum. Metamask functions as a Web3 wallet that can generate and govern user identities. It connects the user to the Ethereum network. It administers the web3.js library into the search engine to authorize read and write requests to be executed on blockchain networks, like Ethereum by designating an external method called URL.

B. Ganache

Ganache is a personal blockchain network for compact Ethereum application development. Ganache can be used across the entire implementation cycle; allowing the user to develop, deploy, and test various decentralized applications in a controlled and deterministic environment. Ganache controls the blockchain functionality by examining the conditions of the user system. It provides visual mnemonic information and account addresses.

C. *Ethereum*

Ethereum issues a decentralized machine, known as the Ethereum Virtual Machine (EVM), which has the capability to implement code using a global network of shared nodes. Ethereum was instituted in the year 2015. Ethereum can also share the peer-to-peer networking module that makes it distributed. Ethereum also produces its own crypto-currency called 'Ether'. Another feature of Ethereum is that it provides a platform where smart contracts can be created with the help of Ethereum's own language called 'Solidity'.

D. *Remix - Ethereum IDE*

Remix may be defined as an open-source suite of tools that aids smart contract development and deployment which also works as a core of native plugins of Remix IDE. It enables the user to write smart contacts directly from the internet browser. Remix is written in JavaScript and supports both local and native browser usage. Remix also supports contract testing, debugging and deploying.

E. *Smart Contracts*

A piece of code that is used to perform any operation on the blockchain is known as "Smart Contract". Since smart contracts run on the blockchain network directly, it's not possible to tamper or alter the private data. Smart Contracts are run when users send transactions. Smart Contracts are scripted using the Ethereum language, solidity. After programming the needed operations the programmers can compile them by using Truffle which is elucidated in the below section.

F. *Truffle*

Truffle is a development environment focussed on Ethereum development. It also consists of a testing framework and an asset pipeline which aims to make Ethereum development exponentially easier. Truffle has smart contract compilation capabilities built in to aid contract development. The console of Truffle directly communicates with smart contracts.

G. *Mongo-DB*

MongoDB is a document-based ,cross-platform, database application, which is a general-purpose, distributed database constructed for modern implementation of systems and it is also used in cloud storage technology. Each database contains collections which successively contains loads of different documents. Each of the documents is often quite different with a varying number of fields. The size and content of every document are often varying. Sand is rarely constant.

IV. IMPLEMENTATION AND SYSTEM DESIGN

The related work section expounded above includes the work done in the implementation of electronic healthcare facilitating blockchain technology. The paper provides certain solutions in resolving existing problems in Blockchain Technology. The proposed system offers to implement a scalable and easy to maintain design which can be deployed in even the most remote areas with ease. Moreover, The implementation of this proposed system uses the Ethereum network. The Ethereum dependencies, as discussed in the related work section of the paper, are also used in building this system.

A. *Design Framework*

In any given system, the Design Framework is the most predominant and pertinent hunk of any framework as it is utilized for the evolution of the network from its thesis. This section highlights the different modules, elements and architectonics that are amalgamated to form the whole system's framework. As seen in the below figure, Fig 1, our proposed system comprises the 3 major elements, the medical institution, the patient and the blockchain. These entities have a supplementary notion which will be elucidated in the upcoming sections.

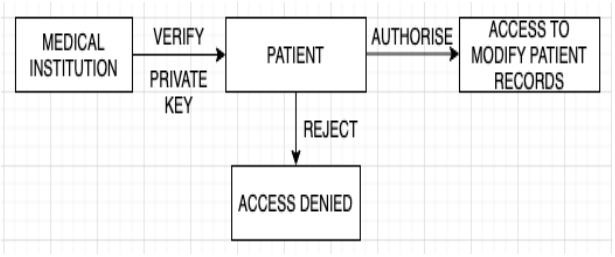

Fig 1. Proposed System Design

A system defines a user as an individual who makes constructive utilization of the system and the allocated resources. A user has various roles and features on the system. For example, let "X" be a patient, who visits a medical institute "A", when X goes to the hospital, all his private medical information or records are uploaded into a safe and secure blockchain network through the help of MetaMask and furthermore it can be distributed amongst other medical institutes, given that all medical institutes are connected to the same network which has been deployed in MetaMask. When X goes to another hospital "B", X need not fill up his medical record yet again, as his record has already been uploaded to the network by A, now, if B wants to access X's medical records, B must send a request to A, once B's request has been acknowledged by A, A can now securely send X's data to B through the said network, but while the transaction is taking place, for the transaction to be successful, A must pay a small amount to MetaMask, known as "Gas Fee", once this is done, the data is securely sent to B, who can now access X's medical records.

B. *System Implementation*

The proposed system was built by implementing Ethereum and a few of its various dependencies. This section aims to provide a clear insight into the working of the system and the various functions it implements.

a) *MetaMask*

Metamask is a browser extension that enables the browser to achieve connectivity to the decentralized web. Transactions done on the Ethereum network require a

certain fee. This is called the gas fee. The amount depends on the amount of computation required to complete the transaction. To put things into perspective, a transaction to create a patient record would attract a gas fee of 0.0000744 ETH, where 1 ether = 150 USD. Metamask also stores the history of the past transactions and hence it would allow the patient to see who all have accessed his/her medical records.

b) Smart Contracts

Smart contracts are an integral part of the proposed system. They are the driving logic which defines the rules and regulations of this system. Smart contracts are scripted employing a language known as solidity. Our system utilizes two smart contracts, namely, HeathRecords and patients.

The 'patients' Smart contract contains the personal details of the patient. It stores details such as the name, phone, email, public key and the age of the patient. It is by utilizing the public key that the patient can authorize and oversee who can access and modify the information.

The 'HealthRecords' smart contract contains the medical conditions and diagnosis of the patient. This contract is mapped to the patient's public key. A medical institution can diagnose a patient with only the public key and hence eliminates and scope of bias in the treatment of the patient.

C. System Functionality

The proposed system is more patient-oriented and the system is built around the preferences of patients and makes sure that the patients have complete rights on their medical records.

The following flowchart, Fig 2, illustrates the functionality of the system. As it is visible from the below figure, Fig 2, there are three important elements involved in the functionality of the system which are illustrated below.

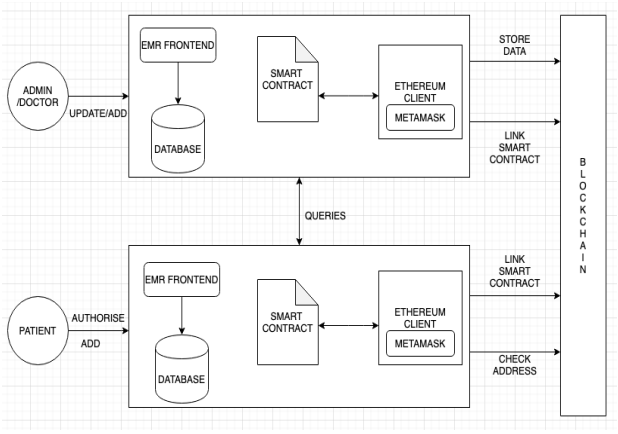

Fig 2. System Operation

Initially, the patient can fill up his medical records digitally and can opt to either keep it confidential and update it himself or share it with medical institutes, if he/she is giving her medical details to a hospital, then it is a direct indication that the patient is authorizing the medical staff of the hospital to collect and update his medical record details when necessary.

Once the patient has accessed his/her account or has created a new account, he/she can then interact with the Electronic Medical Record (EMR) frontend and update his/her name, number, blood group, symptoms, treatments undergoing and more, after updating his account he can submit it. In the EMR frontend, the system provides the user with many options relating to his medical records, for example, the user can modify details about his/her symptoms and the treatments he/she is going through and can update his/her account on such grounds. The user can also add new details regarding his health on the system. Once the user is done updating their account, they can then view their medical records and modify them if necessary. On completion of the aforementioned actions, the user can now add his/her medical record data onto the blockchain network for further use and simultaneously the uploaded data will be deposited in the database. The middleman between the user and the blockchain network is the smart contracts, the smart contracts make sure that the data uploaded is valid and then push the data to the blockchain network, which can be accessed through MetaMask.

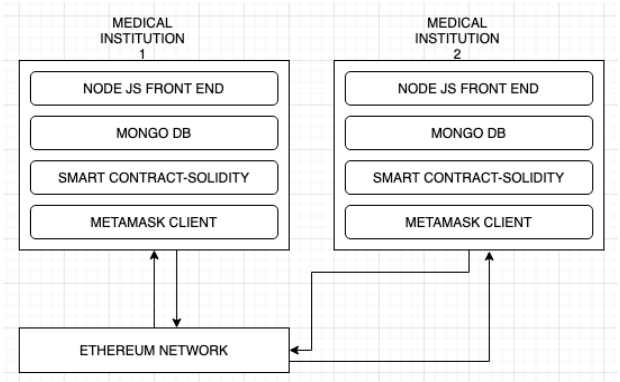

Fig 3. Interaction between two Medical Institutions

Fig 3 elucidates how the interaction between two medical institutions materialize, when a patient uploads his medical records and gives access authority to the hospital, the hospital can now update the patient's data and keep track of the data. If another hospital requests the medical records of said patient, then the hospital can acknowledge their request and send the patient's data through the deployed network in MetaMask, which is hosted using Ganache server. Once the hospital has sent the data to the other, the former hospital must pay the Gas Fee for a successful transaction. Now when the patient goes to either hospital, he/she will not have to fill the medical records again as it has already been shared and any updates done in either of the hospitals on the patient's medical record will be updated on the other hospital's database as well. Each patient record will have a unique public key assigned

to him/her and whenever a doctor has to retrieve the patient's file, he/she can process the public key on the database and can successfully fetch the patient's information.

V. RESULTS

The main objective of this proposed system is to deliver data integrity and quality of data to the patient as well as a stable record management system to various medical institutions. To completely analyze the performance of our system, the solution was tested in various real world scenarios. From the observations made from other related work sections, it is clear that the researched models are more advanced than current models but they also carry some flaws with them, the proposed system works in an efficient way to overcome all the flaws which were observed.

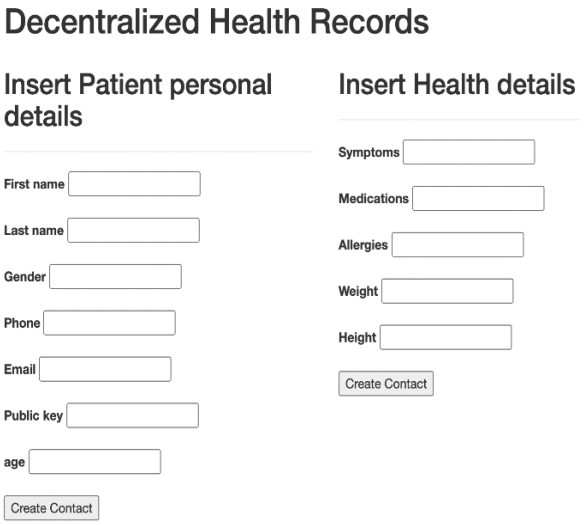

Fig 4. User Interface

Fig 4 illustrates how a patient, medical facility or any healthcare agency can add and update the patient's medical records. In the same way, the patient or the medical institute can delete or view the patient's current medical records.

Fig 5 elucidates on how transactions on MetaMask materializes. The deployer is the origin for sending the data and the address it's directed to belongs to a medical facility or any healthcare agency. It is observed that the gas fee is consumed when a smart contract is deployed to the decentralized network.

The proposed system also gives the user to access his/her previous transactions and make sure they have been sent successfully and are valid. The Transactions hold many important data such as Transaction hash, Transaction Index, Gas details and the smart contract status, Block Hash, Block Number which can be accessed and viewed in the terminal using Truffle.

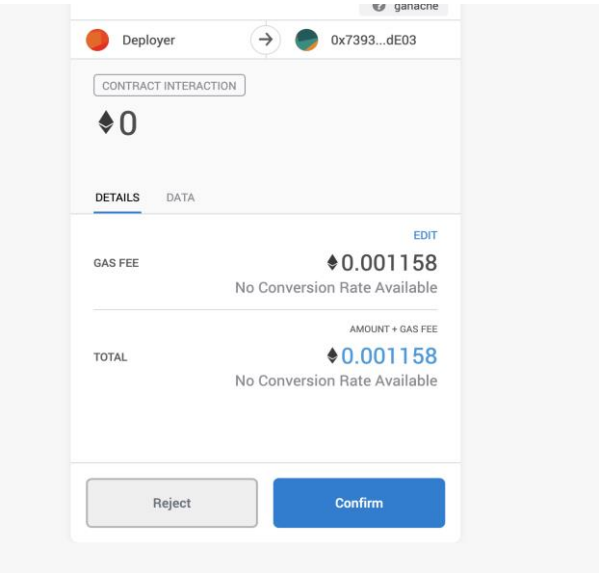

Fig 5. MetaMask Transaction

Fig 6. Transaction Details

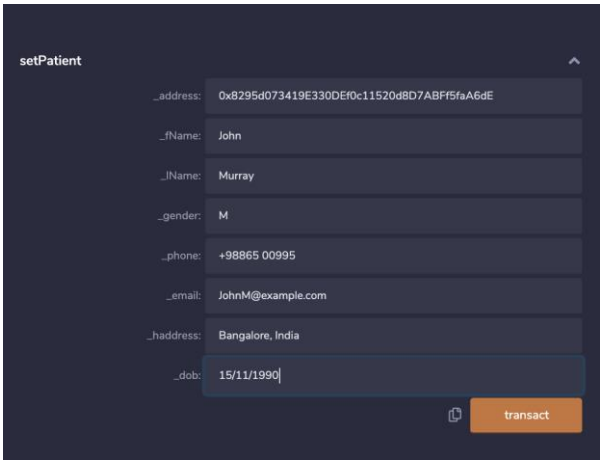

Fig 7. Debugging the patient's Smart Contract

Fig 8. Encrypted Patient Input

Fig 9. Decrypted Patient Output

The series of figures Fig 7, Fig 8 and Fig 9 explains how the patient can input their private data and the following figures show how the private data is encrypted and decrypted from end to end. Each patient record will be assigned to a unique public key which can be used by the medical facility staff to retrieve the patient's data.

Fig 10. Patient Data Retrieval

As it can be seen in Fig 10, each patient will be assigned his/her own unique key which can be used to access his/her data in the blockchain network and the database of the medical facility. By using the patient's unique public key, the staff will be able to retrieve a particular patient's data and work on it if necessary or for reference. The patient can authorize who can access his/her personal details and restrict the authority to only the staff of the medical institution. The data is immutable and cannot be altered once after the patient enters it, ensuring data integrity.

There are a few areas in the implementation of Electronic Medical Records where the proposed system stands out. The following table, Table 1, compares the proposed system to the existing systems.

Related works comparison				
	[1]	[6]	[3]	Proposed system
Blockchain Based	YES	YES	YES	YES
Ease of Deployment	NO	YES	YES	YES
Scalability	YES	NO	NO	YES
Access Authorization	YES	YES	YES	YES
Interoperability	NO	NO	YES	YES

Table 1. Comparison with Related Work

There are no "ideal" systems present in the world, consequently, there are drawbacks which are present in our proposed model. Firstly, our system works simultaneously along with MetaMask, Ganache and Truffle, if there is a failure in any of the three applications mentioned above, the system would fall, i.e., Single Point Failure. Secondly, transactions would fail, if the Gas fee is not paid, hence, financing the Gas fee is the only way to make sure that the transaction will be successful. These are the drawbacks of our proposed system.

VI. CONCLUSIONS AND FUTURE SCOPE

The paper has discussed how blockchain technology can be facilitated and used to implement electronic medical records. The system proposed achieves data integrity by making the records immutable and keeping it secure. The patient can authorize who can access his/her records by defining granular access rules for those records. The smart contracts of this system provide a grieving logic of how the system should behave. Although there have been many recent advancements in the electronic medical records sector, with the advancements also comes the loopholes associated with said systems and the designed and implemented system in this paper overcomes all the drawbacks of the conventional models as well as the recent models.

Future work includes the creation of personalized sub-networks within a medical facility which allows the sub-departments in the medical facility to acquire the patient's details and information and update it when necessary. The

hospital can deploy their custom network made in Ganache and connect it to MetaMask. Presently, Gas fee is minimum only in an ideal scenario. In the near future, the model can evolve to drastically minimize gas fee and thus making the system extremely cost-efficient.

REFERENCES

[1] Zhang, Peng & White, Jules & Schmidt, Douglas & Lenz, Gunther & Rosenbloom, S.. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Computational and Structural Biotechnology Journal. 16. 10.1016/j.csbj.2018.07.004.

[2] Kevin Peterson, Rammohan Deeduvanu, Pradip Kanjamala, and Kelly Boles Mayo. 2016. A Blockchain-Based Approach to Health Information Exchange Networks. Proceedings of NIST Workshop Blockchain Healthcare (2016).

[3] Bender, Duane & Sartipi, Kamran. (2013). HL7 FHIR: An agile and RESTful approach to healthcare information exchange. Proceedings of CBMS 2013 - 26th IEEE International Symposium on Computer-Based Medical Systems. 326-331. 10.1109/CBMS.2013.6627810.

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

[5] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma and J. He, "BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange," 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, 2018, pp. 49-56, doi: 10.1109/SMARTCOMP.2018.00073.

[6] Chen Y, Ding S, Xu Z, Zheng H, Yang S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. J Med Syst. 2018;43(1):5. Published 2018 Nov 22. doi:10.1007/s10916-018-1121-4.

[7] Cyran, Marek. (2018). Blockchain as a Foundation for Sharing Healthcare Data. Blockchain in Healthcare Today. 10.30953/bhty.v1.13.

[8] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis and D. Tzovaras, "On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, 2018, pp. 1374-1379, doi: 10.1109/TrustCom/BigDataSE.2018.00190.

[9] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1-5, doi: 10.1109/PIMRC.2017.8292361.

[10] Engelhardt, M. A. 2017. Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. Technology Innovation Management Review, 7(10): 22-34. http://doi.org/10.22215/timreview/1111.

[11] [online] Available: https://truffleframework.com.

[12] [online] Available: https://metamask.io/

[13] [online] Available: http://remix.ethereum.org/

[14] [online] Available: https://www.trufflesuite.com/ganache