IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN TECHNOLOGY FOR PRIVACY PRESERVATION IN HEALTH CARE APPLICATION

[1]Dr.S.Brindha, [2]Ms.G.Amirthavarshini, [3]Ms.K.Rakavi
1 Head of the Department,2,3 Students
[1,2,3] Department of Computer Networking
[1,2,3] PSG Polytechnic College, Coimbatore, India

***Abstract*-**Block Chain is an emerging technology which includes a number of features by default such as, distributed ledger, decentralized storage, authentication, security, and traceability. In health sector, patient data are sensitive and it is very essential to be secured, which can be done using blockchain technology. Exchange of healthcare data between hospitals is limited by privacy and dependency on centralized data management systems. Such a centralized storage can be a concern since it can lead to data leakage, data manipulation, mistrust, and single point of failure. Blockchain offers a decentralized computing and storage solution that can help with these issues. It includes smart contracts, identity verification and more. Integrating block chain technology with identity management will be the solution for some issues, such as centralized governing of identities. This system proposes Ethereum based blockchain data management for healthcare application, to store and review the patient record by web application allowing only identity verified users like patient, doctors, family members and hospital staff to have the secure access to health information. Ethereum currently uses a proof-of-work consensus mechanism. Solidity is the popular language for writing Ethereum smart contracts. The data on Ethereum blockchain is stored using tire data structures to manage temporary and permanent data. To protect data integrity, ownership, and permissions, smart contracts are created. Since the business can be handled by smart contracts, there won't be a need for centralized authority to oversee and authorize it, which will cut costs.

***Index Terms*-Blockchain, Ethereum, Healthcare, Decentralized, Smart contracts.**

1.INTRODUCTION

The healthcare industry is responsible for the management and sharing of sensitive patient information, and privacy concerns have always been paramount. Traditional methods of data management, such as centralized databases, have proven to be vulnerable to data breaches and cyber-attacks, resulting in significant losses of patient data. In response to these concerns, blockchain technology has emerged as a promising solution for privacy preservation in healthcare applications. Blockchain is a distributed ledger technology that maintains an unchangeable record of all transactions made on the network. Each transaction, or block, is verified by a network of participants before being added to the chain. This process ensures the integrity and confidentiality of data stored on the blockchain. Blockchain technology can provide a secure and transparent platform for patients to manage their health data and control who has access to it, all while maintaining their privacy. One of the main benefits of blockchain technology in healthcare is the ability to maintain the confidentiality and integrity of health data. By providing a decentralized platform for data management, blockchain can minimize the risk of data breaches and cyber-attacks, which can result in the loss or theft of patient data. In addition, blockchain can enable patients to control their health data, providing them with greater transparency and autonomy. However, the implementation of blockchain technology in healthcare also poses challenges. One of the main challenges is interoperability, as different healthcare providers often use different systems and standards for managing patient data. Additionally, blockchain technology must comply with strict regulations such as HIPAA and GDPR, which require strict controls over how patient data is stored and shared. Despite these challenges, blockchain-based healthcare startups have emerged in recent years. These companies are developing platforms to address the challenges of interoperability and compliance while also providing patients with greater control over their health data. Some examples include in Health. In conclusion, blockchain technology has great potential for privacy preservation in healthcare applications. Its ability to maintain the confidentiality and integrity of patient data can improve patient

outcomes and empower patients to take control of their health data. While there are still challenges to overcome, the emergence of blockchain-based healthcare startups is a promising sign of the technology's potential.

II. LITERATURE REVIEW

For the storage and transmission of medical data, scholars around the world have conducted a lot of researches. In 2012, Patra proposed a cloud-based model to process private data for patients. Through his framework, medical personnel and policy makers can use the cloud-based model to provide remote medical services to patients. This model stores all necessary data in a single cloud. By encouraging patients to share data in the cloud, patients can obtain medical staff services. Disease diagnosis and control can be performed through remote treatment. In 2014, Ye proposed a well-organized authentication and access control scheme based on the attributes of the perceived IoT access control layer.
In 2015, Ziskind proposed a privacy preservation platform, which uses third-party equipment to provide services and allows users to modify authorization while following the access control policies reserved on the blockchain. The proposed decentralized platform contains three objects: service providers, mobile phone users, and nodes that maintain the blockchain. Two types of transactions can be defined in the blockchain network in the platform: Data for data storage and recovery and access time and Tacks for access control management. The data collected through the user's mobile phone is encrypted and saved outside the blockchain. In the public chain, only data hashes are saved. Both users and services can query the data in Data transactions. In 2016, to solve the problems of slow medical record information access, data fragmentation, and user privacy preservation, Azaria completed a medical data sharing platform based on Ethereum. Peterson et al. proposed a blockchain-based participant in advance. A medical data sharing plan with a well-defined rule structure is agreed. Although this solution realizes the sharing of medical data, it lacks a universal access control strategy.

In 2017, Omar proposed data management system for patient healthcare. By adopting blockchain to protect privacy storage, it solves the problem of losing control when storing encrypted data in the system. In addition, by using encryption on the blockchain, the framework will not be affected by data preservation vulnerabilities. Do and Ng proposed a system that uses blockchain technology to provide secure distributed data storage with keyword search services.

In 2018, Magyar designed an integrated health information model that builds a decentralized and openly scalable network based on the blockchain operating environment, making access to data more secure. In order to handle the protected health information (PHI) generated by these devices, Griggs proposed utilizing blockchain-based smart contracts to facilitate secure analysis and management of medical sensors. Using a private blockchain based on the Ethereum protocol, they created a system where the sensors communicate with a smart device that calls smart contracts and writes records of all events on the blockchain. This smart contract system would support real-time patient monitoring and medical interventions by sending notifications to patients and medical professionals, while also maintaining a secure record of who has initiated these activities. This would resolve many security vulnerabilities associated with remote patient monitoring and automate the delivery of notifications to all involved parties in a HIPAA compliant manner. Liang proposed an innovative user-centric health data sharing solution, which uses the blockchain mechanism to protect privacy, strengthen identity management, and collect data in conjunction with mobile applications.

Zhang and Lin proposed a personal health record sharing scheme based on blockchain. This solution builds two different blockchains to realize the safe sharing of medical data. The plan separately builds a private chain and a consortium chain. The private chain realizes the encrypted storage of personal medical data. The consortium chain saves the security index corresponding to the personal medical data and secures the data sharing by verifying the doctor's identity token, which protects the medical data. However, using two types of blockchains will not only increase costs, but also reduce their execution efficiency. Ji investigated the location sharing based on blockchains for telecare medical information system. Firstly, they define the basic requirements of blockchain-based location sharing, including decentralization, unforgeability, confidentiality, multilevel privacy preservation, retrievability, and verifiability. Then, using order-preserving encryption and Merkle tree, they proposed a blockchain-based multilevel location sharing scheme.

In 2019, Wang combined homomorphic encryption and proxy encryption technology to implement outsourcing computing solutions in healthcare systems. In this solution, there are several clients with different public keys, an electronic medical cloud platform, and an auxiliary cloud server. The electronic medical cloud platform can provide services to patients and regularly analyze data to provide better services. The HGD architecture based on blockchain proposed by Yue enables patients to safely control and share medical data. Aiming at the privacy of medical data, Tian proposed to establish a shared key that can be reconstructed by legitimate parties before the diagnosis and treatment process begins.

At present, a large number of excellent schemes have emerged in mobile medical, and their security and flexibility have been continuously enriched. The characteristics of activity and diversification can better meet the needs of practical application, but there are still some deficiencies. Some schemes encrypt the patient information and store it on the blockchain, and some schemes use anonymous certificates to protect user information. But the doctor cannot read the relevant information. Therefore, it is necessary to design a scheme that can authenticate the device.

III. PROPOSED SYSTEM

This proposed system aims to utilize Ethereum blockchain technology for privacy preservation in healthcare web applications. The system would enable patients to control their health data while maintaining their privacy and security through the use of smart contracts and decentralized data storage. Blockchain technology is a disruptive technology. Currently, so many real-time applications are being designed using this advanced mechanism. This paper proposes a distributed application-based mechanism for maintaining official medical records. It uses blockchain technology and users as knowledge agents. Initially, the Ethereum was used with MetaMask wallet to the proposed framework to generate medical certificates like
birth, death, and sick.

Furthermore, the system is implemented with a test RPC, Web, and MetaMask to design and deploy the distributed application to maintain the new medical certificates and existing certificates that are available as physical copies. Logistic Map Encryption function is used to generate cipher medical certificate of existing physical copies to maintain over a blockchain. So many applications have been proposed in the health sectors using blockchain. Some of the lapses existing in the proposed work are lack of implementation results, platform details, etc. The proposed system's main ingredients are authorized health centers as domain experts, users, blockchain as intelligent agents, and local database to maintain the Electronic Health Care

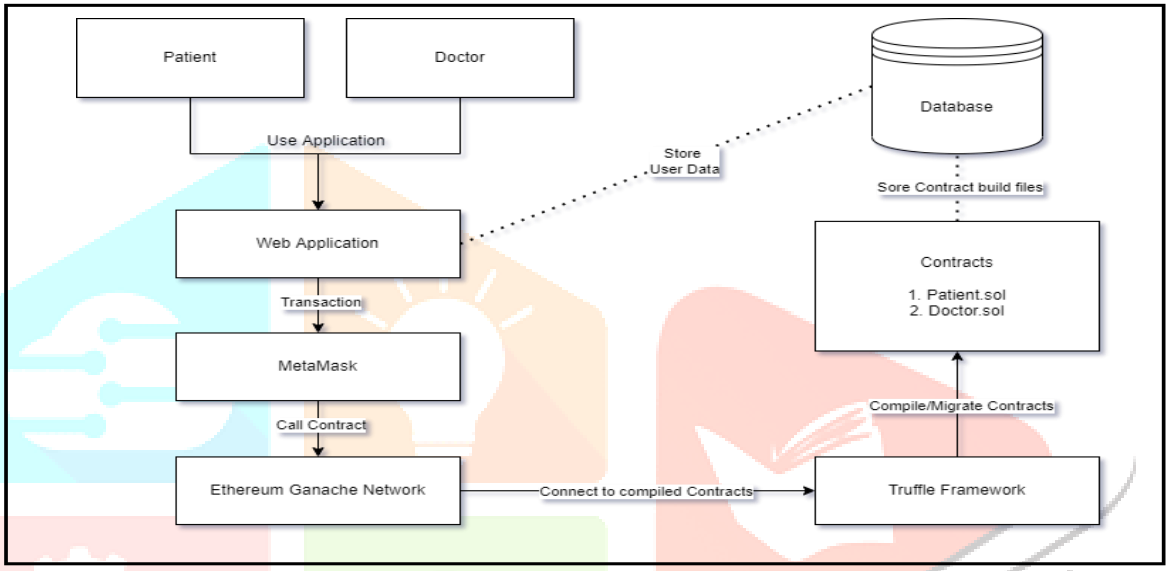

Fig 1. Architecture of a proposed system

IV. SYSTEM ARCHITECTURE

The system architecture of Ethereum blockchain technology for privacy preservation in healthcare web applications involves various components that work together to ensure patient privacy and security. The following is an overview of the system architecture:

Ethereum Blockchain Network:
The system would use the Ethereum blockchain network for secure and decentralized data storage and the execution of smart contracts. The blockchain network consists of a decentralized network of nodes that store a copy of the ledger containing all the transactions and data on the network.

Patient Interface:
The patient interface provides a user-friendly platform for patients to interact with their health data stored on the blockchain. The interface enables patients to grant or revoke access to their data to authorized parties. It also allows patients to view their health data and track any changes made to it.

Smart Contract Engine:
The smart contract engine is responsible for executing smart contracts that define the conditions under which patient data can be accessed. Smart contracts are self-executing programs that automatically enforce the terms of a contract. In the context of healthcare, smart contracts can be used to define who has access to patient data, under what conditions, and for what purpose.

Healthcare Provider Interface:
The healthcare provider interface enables healthcare providers to access patient data with the patient's permission, as defined by the smart contract. The interface provides healthcare providers with secure access to patient data, enabling them to provide better and more efficient care.

Decentralized Data Storage:
The system uses decentralized data storage to ensure that patient data is stored securely and redundantly. Decentralized data storage involves storing data across multiple nodes on the blockchain network, ensuring that data integrity and redundancy are maintained.

Privacy-Preserving Techniques:
Privacy-preserving techniques are used to protect patient data from unauthorized access. The techniques can include advanced cryptography, such as homomorphic encryption, that enables computations to be performed on encrypted data without the need for decryption.

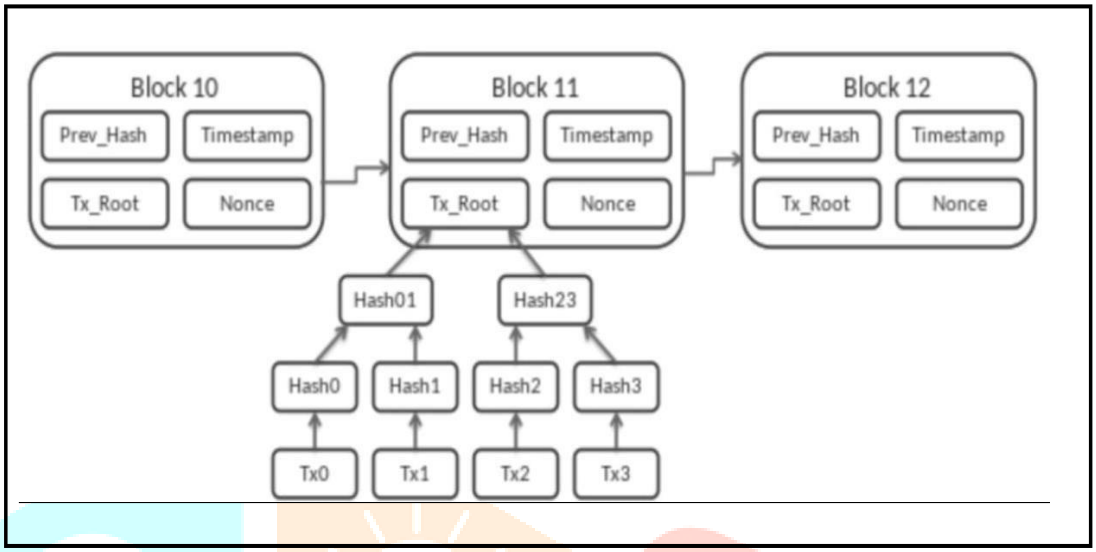

Fig 2 Hash block

V TESTING AND RESULT

We have implemented the proposed system using the remix platform and tested it using the test platform. Ethereum blockchain network is used in these platforms. Moreover, this system used a browser extension, MetaMask cryptocurrencywallet, to deploy the system operations over a blockchain network.

An open-source, public blockchain-based application, Remix is used here to write the smart contracts using solidity programming for the functions performed by theproposed system. Furthermore, we have deployed the proposed system operations using a decentralized application designed using Web, Test node, and solidity programming based smart contracts.

Type	Signature
Lattice	Falcon

Table 1 Type and signature

Algorithm	CPU ±CI
Falcon 512	29.84% ±0.47%
Falcon 1024	31.43% ±0.61%

Table 2 CPU usage of Algorithms

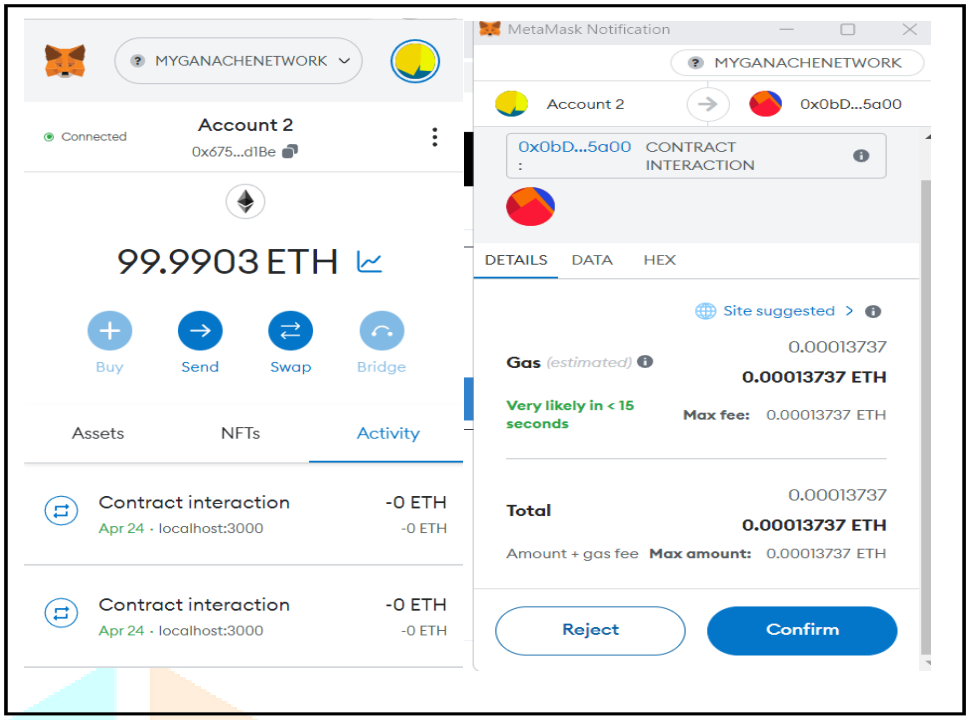

Fig 3 Imported account and confirming transaction

We have to pay a crypto balance to operate any function over a blockchain network. show the confirmation request screens to establish a connection with the operating costs. The credentials enter on the webpage verified with the details in the Google Firebase at administration side.

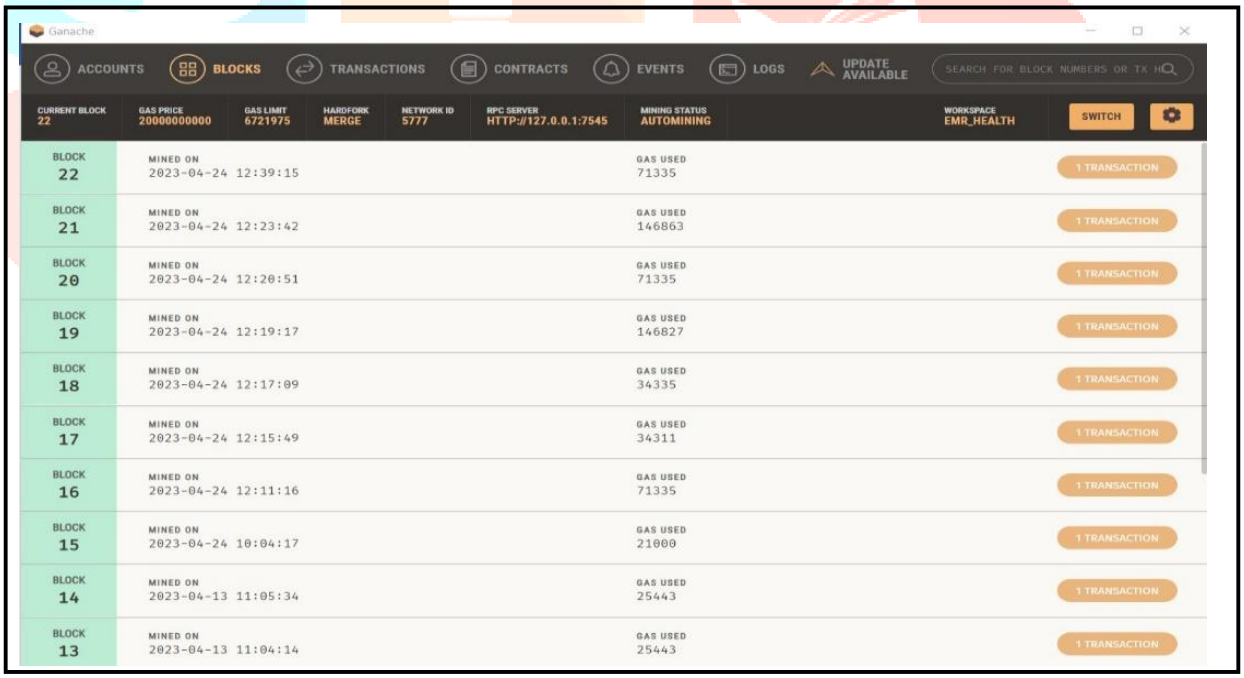

Fig 4 transaction

Figure 4 shows the details of transaction hash, block number, from address,to address, the value of the transaction in terms of Ether, TX Fee, Nonce, etc. The proposed system performance analyzed by considering the existing systems by considering the non-functional operations such as latency and processing time.

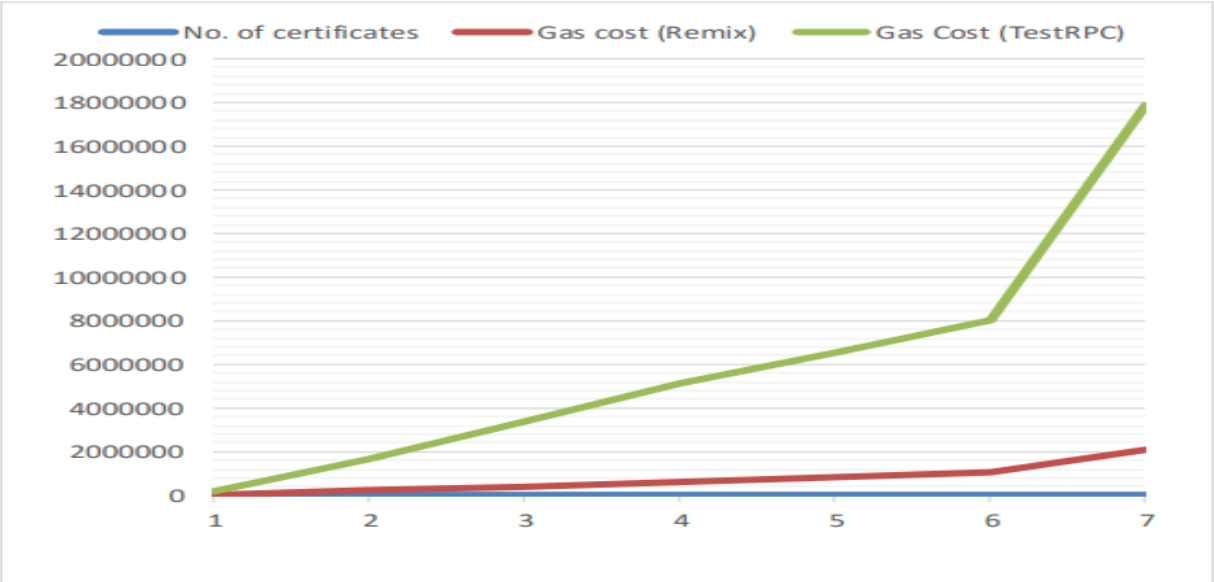

Fig 5 Gas cost to set the medical certificates credentials on various platforms

Figure 5 shows the details of transaction hash, block number, from address,to address, the value of the transaction in terms of Ether, TX Fee, Nonce, etc. The proposed system performance analyzed by considering the existing systems by considering the non-functional operations such as latency and processing time.

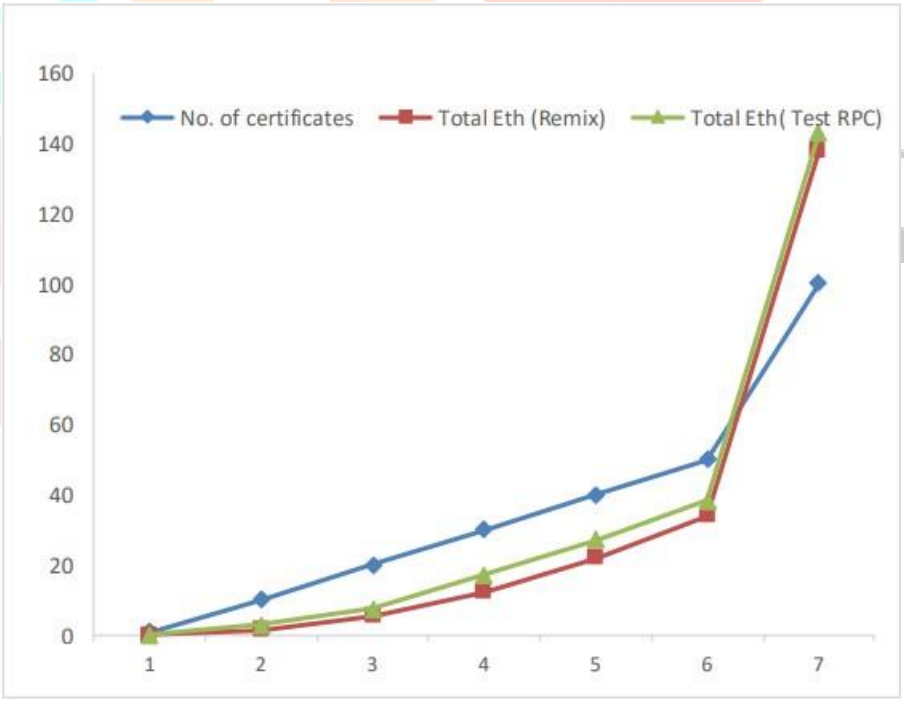

Fig 6 Consumption of total Eth for certificates generation

Figure 6 shows Gas's consumption to generate medical reports on both the platforms such as Remix Ethereum blockchain and test Ethereum blockchain using MetaMask Wallet. Gas consumption is measured in the units of Eths Here we tested the application by generating up to 100 certificates.

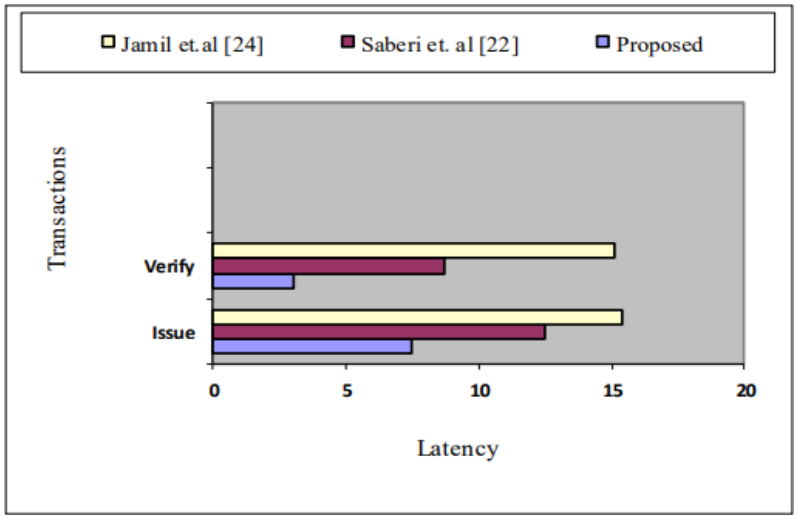

Fig 7 Latency time for different transactions.

Figure 7 shows the details of the proposed system's operational cost on the network and the localhost 8545 network by Web-based distributed application andremix-based system application.

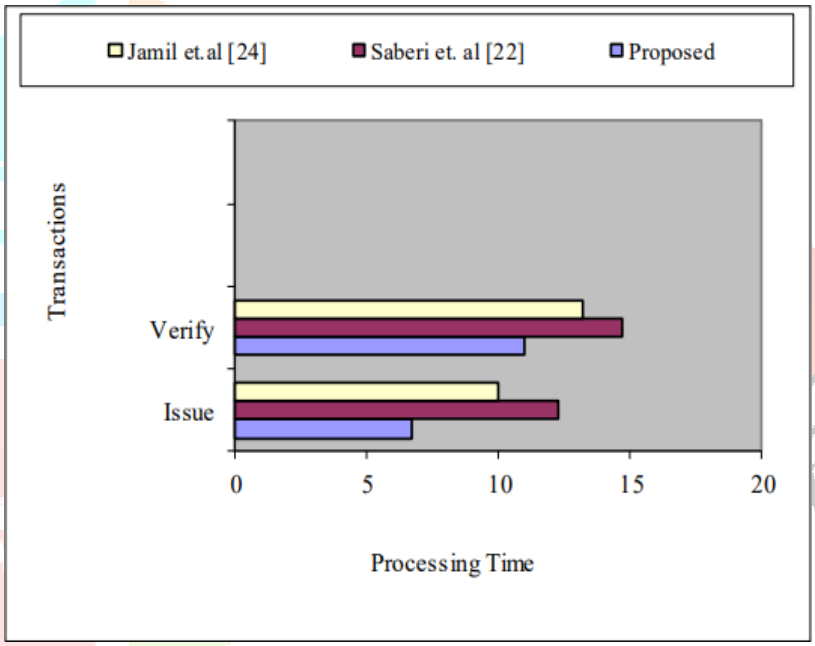

Fig 8 Processing time for different transactions

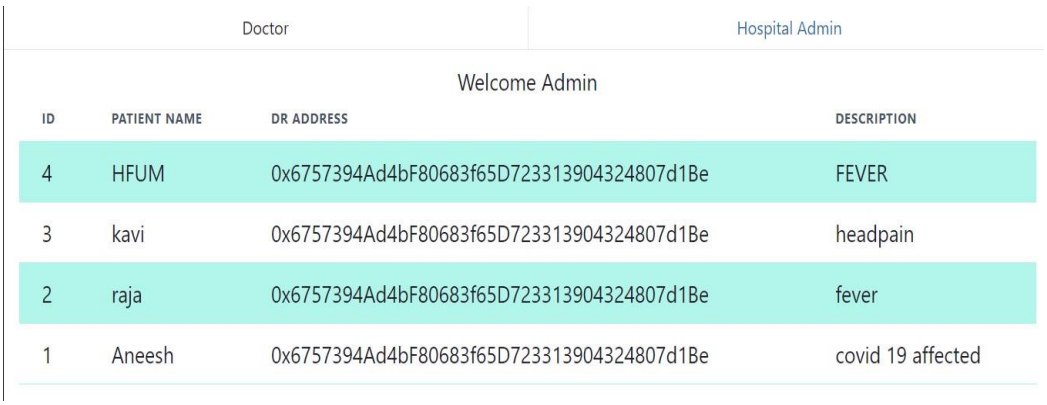

Fig 9 Hospital admin

After the transaction of doctor to patient details in the hospital admin we canable to view the details of patient report by the website

VI. CONCLUSION

Blockchain technology can help reduce fraud in the distribution and management of medical certificates. The proposed system will automate the certificate generation and certification process and maintenance and make it an attack resistance system using Ethereum based public blockchain technology. A single point and Central Authority failure affect the reliability of the system. The proposed approach reduces these kinds of problems with the immutable feature of the blockchain.

7025 Mathematical Biosciences and Engineering Volume 18, Issue 5, 7010–7027. Due to its transparent feature, every node in the system gets information about creating a new medical certificate in a block as a transaction. Here Mata mask wallet is used for cryptocurrency balance in terms of Eths to operate system functionalities over a blockchain. The proposed system is a user-friendly application to issue or verify medical certificates from anywhere at any time

REFERENCES

[1] M. Tabrez Quasim, F. Algarni, A. Abd Elhamid Radwan and G. M.M. Alshmrani,"A Blockchain-based Secured Healthcare Framework," 2020 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2020, pp. 3391, DOI: 10.1109/ComPE49325.2020.9200024.

[2] Zhang M, Ji Y. 2018."Blockchain for healthcare records: A data perspective".PeerJPreprints6:e26942v1 https://doi.org/10.7287/peerj.preprints.26942v1

[3] Chen, Y., Ding, S., Xu, Z. et al "Blockchain-Based Medical Records Secure Storage, and Medical Service Framework" J Med Syst 43, 5 (2019). https://doi.org/10.1007/s10916-018-1121-4

[4] N. Kshetri,"Blockchain and Healthcare Records," in Computer, VOL. 51, no. 12, PP. 59-63, DEC. 2018,Doi: 10.1109/MC.2018.2880021

[5] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella,"Ancile: Privacy-preserving framework for access control and interoperability of health records using blockchain technology," Sustain.Cities Soc., vol. 39, no. August 2017, pp. 283–297, 2018.

[6] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman,"MedRec: Using blockchain for medical data access and permission management," Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016,pp. 25–30, 2016

[7] D. Ouagne, S. Hussain, E. Sadou, M. C. Jaulent, and C. Daniel, "The Healthcare Record for Clinical Research (EHR4CR) information model and terminology," Stud. Health Technol. Inform.,vol. 180, pp. 534–538, 2012.

[8] The IBM Advantage for Implementing the CSCC Cloud Customer Reference Architecture for Blockchain," 2017.