Medical Image Data with Secure Data Storage System Using Block Chain

¹DONDETI RAM MOHAN REDDY, ² BOSU BABU K

¹Associate Professor, Mtech, Newton's Institute of Engineering, Macherla.

², Mtech Student, Newton's Institute of Engineering, Macherla.

Abstract: *Many images of the patient are created every day in the medical field, including ultrasound, CT, X-ray, and more. Medical information is related to the privacy and privacy rights of the people concerned. Therefore, the security and confidentiality of the scientific evidence is very difficult. In order to comply with the guidelines of the Data Protection Act, medical images must be covered in a friendly manner. Therefore, we have prepared a reliable chest x-ray image from Kaggle, mainly based on block chain technology. We created a smart contract to fully control, on location, the permission to access and analyze the research images. We have done cryptography work on the X-ray image after each diagnosis and stored the fingerprint of the image in the block chain. Artificial intelligence has been used to understand diseases related to lung cancer. We compare the X-ray recovery time required with conventional PACS models. The test results confirm that the cost of the request for the use of block chain will be around 5%.*

Keywords—medical image data, block chain, smart contract, Dapp.

I INTRODUCTION

Various images of the patient are created every day in research programs such as ultrasound, CT scan, X-ray, etc. Due to the rapid development of the information age, big data is required [1]. Since medical information is related to privacy and individual rights, the security and confidentiality of research images are very important. However, the station's medical record still relies on the vehicle's central medical record (EMR). In order to comply with the provisions of the Privacy Act, research images must be covered by security measures. With this in mind, we proposed a parking system for medical image analysis entirely based on block chain technology.

In addition to simple data storage, block chain is used to store data through encryption techniques. [2] When a node

makes a transaction, different nodes start validating. This transaction is defined when the number of verification has reached more than fifty-one percent of all nodes [3]. In this case, each change in information on the block chain is guaranteed by strict and comfortable technology. Since the modification is carried out under the quality verification certificate, the specific impurity data may be affected or modified illegally. With this in mind, we used the proposed method of using the Ethereum token agreement [4]. We created a block chain- When searching for images, all data is stored, making the image statistics of the data subjects more secure.

II BACKGROUND KNOWLEDGE

A. Block chain

Block chain is a distributed ledger. The participants are connected by the community together and all the information is shared in the report. It has two roles: the node and the money node [4]. Ordinary nodes are used for business and different transactions, while accounting nodes are responsible for accounting services and managing ledgers. The data linked by the block chain allows both parties to record the complete transaction, and the content of the transaction can be queried and demonstrated. The block chain ecology is constantly

evolving and it is widely used for Bitcoin and different exchange currencies which is 1.Zero block chain. Block chain 2.Zero specializes in the development of "smart contracts", which refers to the technology developed by Ethereum [5]. 3.Zero block chain gradually emerged after the rise of artificial intelligence (AI) technology [6]. The device used in this research is an Ethereum smart contract that belongs to the 2.Zero block chain.

The features of block chain are briefly explained as follows.

◆Decentralized database: information is created and exchanged between them.

Peer-to-peer connection: Nodes can communicate, store and send statistics to each other at once.

Anonymity and transparency: customers are identified using a number of more than 30 characters and remain anonymous.

◆ Unqualified: Once the true data of a transaction is recorded, they will be stored permanently and cannot be changed.

◆Logical Algorithm: Users can modify the process for starting the business of machines. In a block chain system, each block is uniquely correlated to each other. As long as the content of one of the blocks changes, it wants to be displayed again, and the same goes for the new blocks. There is a lot of information in each block, including the peak block label, previous block hash value, current block hash value, total (unlike)

estimated value, timestamp, hash value of transaction points and transaction points to be trusted. that the data is fair [7,8]. For data security, transaction details are hashed twice in each block. In this research, the image data is first transformed by hashing and then put into the block chain, just like the security of the study data. In addition, regarding the verification process at the block chain level, each of these is used to compete to calculate the total stake value (not) of the new product. To ensure the correctness of the content in the block, the amount of evidence must exceed 51% of all nodes. The image of the block chain is shown in Figure 1.
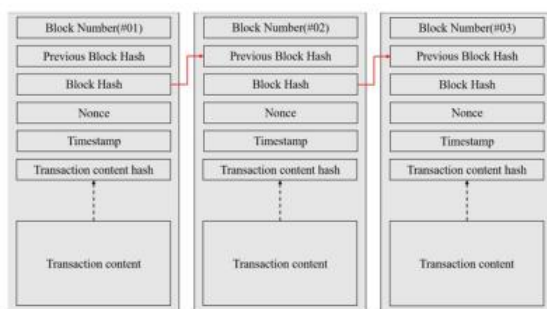

Fig. 1. Block chain structure.

B. Smart contract

Ethereum, a block chain platform launched in 2015, was renamed "Next Generation Smart Contract and Decentralized Application Platform" in its white paper. Although smart contracts were proposed by Nick Szabo in the early 1990s, they did not have much time until Ethereum was promoted again and brought them to many places, or even became "Block chain 2.

Zero" [9]. The areas where smart contracts are used are financial markets, weather forecasting, flight control, for ex and billing where applicable.

C. Electronic medical record (EMR)

Electronic medical records (EMR), in view of the fact that Article 69 of the "Medical Law" was amended on January 29, 2013, has ended for Taiwan's famous hospitals. Although it is very inexpensive, it helps reduce time, facilitate data analysis, etc. [10,11]. Digital health records are used by doctors to edit digital research data after examining a patient and send associated medical tests such as x-ray photos. Medical data is transferred to the host PC of the medical center. If the data is accessed for medical records purposes, it must be transmitted via the owner's laptop according to the appropriate rules. Its operating diagram is shown in Figure 2.

*PACS: Picture Archiving and Communication System
*EMR: Electronic Medical Record
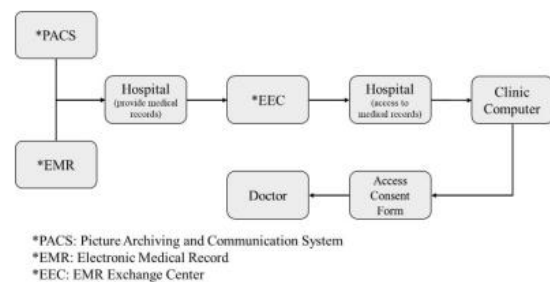*EEC: EMR Exchange Center

Fig. 2. Electronic medical record.

D. Picture Archiving and Communications System (PACS)

The function of the entire EMR gadget is dedicated to storing and transmitting patient data, Images Archiving and Communication System (PACS). In this

equipment, after receiving the photo data including X-ray, the photography and conversion is done. To coordinate with the EMR system, the image is converted to DICOM (Digital Imaging and Communications in Fashion) Service-Object Pair (SOP), and then operations such as saving, recalling and exporting can be performed. . They are evident in Fig. 3 and 4, do.
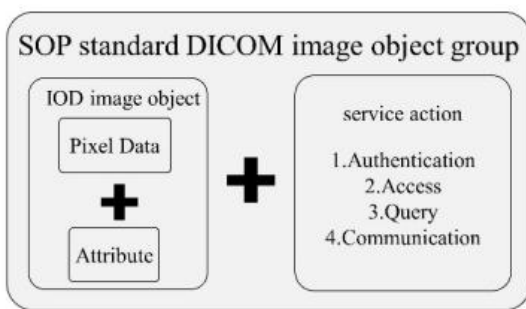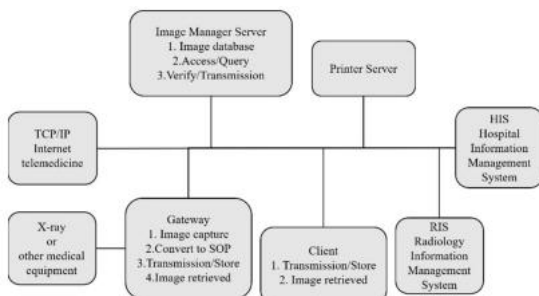

Fig. 3. SOP standard DICOM image object group.

Fig. 4. Picture Archiving and Communication System (PACS).

III RESEARCH METHODS

To improve the security and integrity of the existing PACS, advanced functions are planned as follows: writing smart contracts to confirm the authorization function, sending recommendations to the block chain, performing a hash change on the image file and 'send to the block chain. .

A. System development platform

1) Nod.Js

Now maintained by the Open JS Foundation, node.Js is a cross-platform, open-source working environment for running server-side JavaScript. It takes a lot of work and makes it easy to improve the usefulness of the website. He has many special abilities. All users use the network server, and the "asynchronous I/O" operation does not delay scheduling and enables 0.33 day birthday modules with less power consumption.

2) Potatoes

Truffle is currently the main development of Ethereum. Its development language is JavaScript to support the compilation, deployment and analysis of smart contracts. When creating smart contracts, JS or Solidity is used to draft and support. Truffle manages the transfer between the public chain and the private chain.

Truffle is the easiest way to use the command line in Windows to run the command "$ npm install truffle -g" after Node.Js installation is complete to complete the installation. Once the installation is complete, it continues with the following command. "$mkdir Dapp_xray" to create a new Dapp_xray folder, "$cd Dapp_xray" to move the path to the Dapp_xray folder and "$truffle init" to start a new Ethereum target. After completing the instructions above, the file will appear in the Dapp_xray folder.

Then 3 Solidity files are created in the contract, which can be xray.Sol, xr.Sol and strlib.Sol. Xray.Sol is the contract of the X-Ray contract, defines the realm variables, enumeration (enum), structure (struct), modifier, time (event) and internal nature of the ability. Xr.Sol is an X-Ray contract, providing plenty of power to run the program, as well as Get, Set and Remove functions. Strlib.Sol is a string library. After writing the contract, 1_initial_migration.Js is run in the migration folder to configure the settings required for deployment. The locations are shown in Figure 5. Once the installation is complete, the following instructions are complete.

"$truffle bring Together" compiles the smart contract.

```
const strlib = artifacts.require("strlib");
const xr = artifacts.require("xr");

module.exports = function(deployer){
  deployer.deploy(strlib);
  deployer.link(strlib, xr);
  deployer.deploy(xr, 'Ken',
'0x483845112c9B815a5B443bd3aDc2bD6e0D6e0D573ce5', 25, 0, 1);
}
```

Fig. 5. Related settings before deployment.

When the compilation is complete, truffle-config.Js defines the relationship with the block chain. The contents of the site are linked to the Ganache package. Once installed, the following command is executed. "$truffle migrate" sends smart contracts.

3) Ganaches

Ganache started the virtual Ethereum block chain and together with the Truffle suite delivered in the previous phase to run the digital measurement. Ganache simulates the Ethereum block chain and developers don't want to install nodes. He sees the glory, the place, the importance, the change and the stability of everything today. Log output from the internal block chain will also be taken into account every time and configure a special mining field. After going through the Truffle Deployment Agreement order in the previous section, the remaining node money of Ganache began to be traded and sold.

B. Operating Procedures

Figure 6 shows a schematic diagram of this device. The front-end component is based on the main medical picture storage and transmission system (PACS) running, and the rear module converts the system by hashing and passing the proof of the intelligent communication. said fit. Finally, the image is uploaded to the block chain.
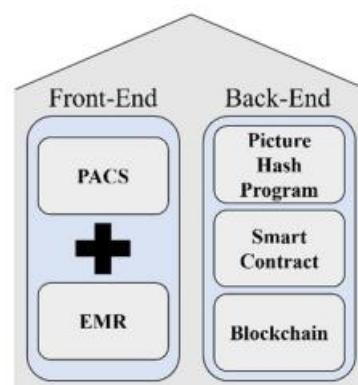

Fig. 6. System architecture.

In this gadget, the role of the Meta Mask is to record the block chain debt and provide

users with a place to report all transactions. After registering the Meta Mask, the user enters the settlement for authorization verification (Fig. 7). Since smart reconciliation allows all documents in the sanatorium to prove the authorization of these devices, the account protects the doctor against the responsibility. Instead, he is far more isolated as a patient and has the right to ask for medical information.
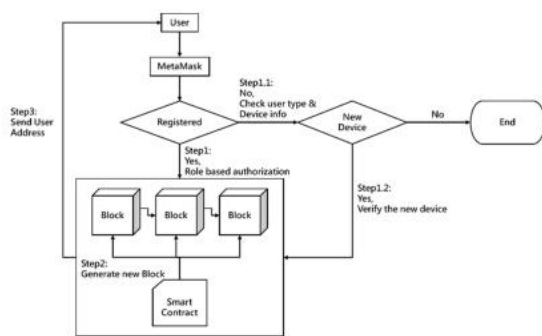

Fig. 7. Users registration process.

In addition, after the registration is completed, both patients and doctors can query the image data. However, the block chain is only used in this system to ensure the security of data storage. In the query process shown in Fig. 8, doctors can check the data with the doctor after the patient obtains the hash value of the imaging data given by the doctor.
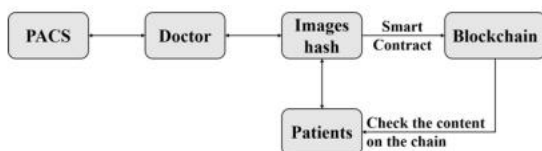

Fig. 8. Image data query/check process.

IV IMPLEMENTATION AND ANALYSIS

Truffle commands are used to complete the smart contract deployment and then perform per-authorization and authentication tasks. Additionally, the hash value of the X-ray image of the interceptor must be obtained before processing. For an experiment, we use the Kaggle-defined chest x-ray image statistics shown in Figure Nine. We use Python to write an application that converts images into hash values added to the device. The performance results are shown in Figure 10.

Fig. 9. Chest X-Ray images.

Fig. 10. Hash value of patient's X-Ray image.

A. Pre-work

After the deployment was completed, we typed the following command to enter the console mode to behavior the simulated transactions: >truffle console. To transfer bills to initiate transactions at any time, we declared the variables to install all money owed: >permit debts. Then, we used the built- in web3.Js function library within

the console mode, which changed into a characteristic library normally used by DApps to question accounts and conduct operations such as

>web3.Eth.GetAccounts(function(err,res) debts = res;).

For comfort, we saved the number of declared edges into the corresponding variable.

>let gov = debts[0]

>permit host = bills[1]

>permit physician = accounts[2]

In this manner, all account addresses inside the variable money owed had been described. Finally, the smart settlement was acquired, and the clever contract xr turned into declared as xry.

>let xry

>xr.Deployed().Then(instance => xry = instance)

B.Permission Setting

For permission placing, Dr. Lee's authority was given. The "1" within the command line refers to the medical doctor within the User Type enumeration: >xry.Set Permission(health practitioner, 'Dr.Lee', 1, genuine)

C. Data Setting

After putting permissions, Dr.Lee's account is used to installation Ken's examination image statistics. We took the chest X-Ray pics for example for the experiment. The instructions for setting the patient image statistics are as follows. The parameters inside the command line are the inspection web page and the hash fee of the image.

>xry.SetXrayhash('chest', '16c8a694c91b80f1d97efb91455ab8b3fac d6221ea401d7400   86722d4bad0134', from: medical doctor)

Then, the host account is used to set up the birthday (birthday) and call facts (contact) within the non-public information, the command traces are as follows. The first line is for placing the birthday and the second is for the touch statistics.

>xry.SetBirthday('19970522', from: host)

>xry.SetContact('0912-321-456', from: host)

D. Query Data

After the above settings are finished, we queried the patient's photo-related information. The command line to query the patient's fundamental records become as follows.

>xry.Profile()

Before querying the photograph data, the array field have to be obtained first the use of the subsequent command traces.

>xry.GetXrayhashCount()

>xry.GetXrayhash(zero)

After the above two instructions, we carried out the command to query the picture records. The query command and the end result are shown in Fig. 11.

```
truffle(ganache)>x.getXrayhashCount()
BN { negative: 0, words: [ 1, <1 empty item> ], length: 1, red: null }
truffle(ganache)>x.getXrayhash(0)
Result {
  '0': 'Dr.Lee',
  '1': 'chest',
  '2':
'16c8a694c91b80f1d97efb91455ab8b3facd6221ea401d740086722d4bad0134'
}
```

Fig. 11. Query the patient's image data.

E. Permissions Remove

When medical doctors resign, their authorities are eliminated. After the authority is eliminated, the medical doctor cannot modify the scientific record statistics for the affected person. The education is as follows: >xry.Remove Permission(physician). With the above command, it is examined whether the permission has been removed. By entering the following command, the photo can't be modified by way of the medical doctor: > xry.SetXrayhash('chest', '16c8a694c91b80f1d97efb91455ab8b3fac d6221ea401d7400 86722d4bad0134', from: medical doctor). Through all the above command operations, users interact

with the device. For example, the patient and the medical doctor can question the statistics. After typing the command, the effects are as compared with the EMR machine and the patient's clinical data can be proven.

F. Performance Analysis

In this segment, we illustrate the improvement value and analyze and evaluate the storage performance and safety of our machine. Currently, the system proposed on this examine is more appropriate for small or medium-sized medical establishments. The hardware and software environment for the experiments on this paper is proven in Table I.

TABLE I. EXPERIMENTAL ENVIRONMENT

CPU	Intel® Core™ i7-7700HQ CPU @2.80GHz
Graphics card	NVIDIA Ge Force GTX 1050
Memory	12.0 GB
OS	Windows 10
Block chain (test)	Ethereum (Ganache)
Block chain nodes	10

1) Cost analysis

The design strategy often uses the current PACS to improve data security. In order not to waste time and money, we provide software capabilities in small and medium hospitals. In terms of employee compensation, there is no need to adjust or increase the number of employees.

because it is used on the old system. The most significant additional cost in the system is the virtual transaction fee and the

time required to create a non-public chain. It is also recommended to use the Ethereum Private Chain for installation, and when the installation is complete, the Genesis Block will be used to mine and write Ethereum. This method takes into account the cost of the equipment used for mining. Finally, transaction costs do not require special capabilities or protection, but the routine operation of nodes to ensure that the non-public chain can exchange and store information usually.

2) Auditing time

Figure 12 shows the time required for hash conversion and import into the block chain for a specific set of snapshots. When importing into the block chain, the nodes must know each other, so this takes a little time. The control environment of this experiment has become 10 nodes. For example, the download time increased to 56,830 ms and the hashing time to 685 ms with one hundred snapshots.
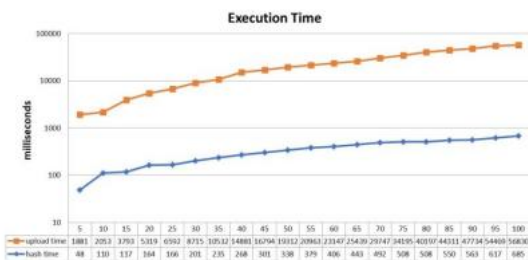

Fig. 12. Hash time & upload time for different numbers of images.

V CONCLUSION

We introduce a new application in the block chain field that combines the high security of block chain with the current widely used EMR gadget to confirm patient statistical images to reduce treatment risks. In the process of proof, the most important role is the authorization of proof. We use Ethereum's consensus technology to solve the human authorization problem and the combination of Truffle Suite and Meta Mask to complete the setup and query in the test private block chain. Scientific statistics simulation and clear display features allow the storage to improve the front-end user interface to make it more user-friendly. For data security and privacy protection, medical snapshots must be included in the security process and comply with the provisions of the Privacy Protection Act. We are known for being a good source of medical information. There are many medical applications to be developed for the use of block chain technology in the future.

REFERENCES

1. Langer, S.G. (2011) Challenges for data storage in medical imaging research. Journal of Digital Imaging. 24, 203–207.

2. Li, R., T. Song, B. Mei, Li, H., Cheng, X. and Sun, L. (2019) Block chain for large-scale Internet of Things data

storage and protection. In IEEE Transactions on Services Computing, vol. 12, no. 5, 762-771, 1 Sept.-Oct. 2019, doi: 10.1109/TSC.2018.2853167.

3. Aggarwal, S. and Kumar, N. (2021) Chapter Twenty - Attacks on block chain working model. Editor(s): Shubhani Aggarwal, Neeraj Kumar, Pethuru Raj,Advances in Computers, Elsevier,Volume 121, 2021, 399-410.

4. Vujičić, D., Jagodić, D. and Ranđić, S. (2018) Block chain technology, bitcoin, and Ethereum: A brief overview, 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 2018, 1-6

5. Chen, J., Xia, X., Lo, D., Grundy, J., Luo, X. and Chen, T. (2022) Defining smart contract defects on Ethereum. in IEEE Transactions on Software Engineering, vol. 48, no. 1, 327-345, 1 Jan. 2022.

6. Silvano, W. F. and Marcelino, R. (2020) Iota Tangle: A cryptocurrency to communicate Internet-of-Things data, Future Generation Computer Systems, Volume 112, 2020, 307-319.

7. Nirjhor, M. K. I., Yousuf, M. A., and Mhaboob, M. S. (2021). Electronic medical record data sharing through authentication and integrity management. In 2021 2nd IEEE International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST) (pp. 308-313).

8. Prasadu Peddi, & Dr. Akash Saxena. (2016). STUDYING DATA MINING TOOLS AND TECHNIQUES FOR PREDICTING STUDENT PERFORMANCE. International Journal Of Advance Research And Innovative Ideas In Education, 2(2), 1959-1967.

9. Prasadi Peddi and Dr. Akash Saxena (2014), "EXPLORING THE IMPACT OF DATA MINING AND MACHINE LEARNING ON STUDENT PERFORMANCE", International Journal of Emerging Technologies and Innovative Research, ISSN:2349-5162, Vol.1, Issue 6, page no.314-318.