A Secured and Decentralized Medical Document Management Methodology using a Private Block Chain.

Shanmugaraja P[1], Soniya Priyatharsini G[2] , Chokkanathan K[3], Senthil Mahesh P.C[4], Vanitha K[5]

[1] Sona College of Technology, Salem, [2]Dr.M.G.R Educational and Research Institute, Chennai, [3] Madanapalle Institute of Technology and Science, Madanapalle ,[4]Excel Engineering College, Namakkal, [5]JAIN(Deemed-to-be-University), Bangalore.

Summary

Creating fake documents and certificates by duplicating them from the real ones has become most popular in the upcoming days. Also, these documents will be stored in their respective offices in a database which is a Centralized Database. Now if we'd like to access them then we should always be physically present in that particular office. Also, during this pandemic, most of the schools, colleges, and offices were subject to online document storage. This blockchain system be in the service of as a solution for the taut storage of documents in the form of electronic files on a blockchain network. The immutable property will aid the document from being duplicated by some other document and also will result in the permanent entry of the particular document in Distributed Databases. Also, the blockchain belongings of the decentralized ledger structure will help to keep the files safe and unaffected forever.

***Keywords**:*

Blockchain, Centralized database, Secure storage.

1. Introduction

Storage of documents has become a very paramount thing in our present way of living. Also, along with this rising needy for documents, the pilfering and duplicating of documents is also increasing day by day. So, there is a very great need for the shielding and authenticating of files to keep them from being demolished, operated, or duplicated into some other file. Also, some documents are so chief in a way that if they are lost, they cannot be rehabilitated or repaired[1]. Apart from all this, the person has to be in-person to visit the appropriate office for restoring their document and this process takes much more time. Because of this, the dominance of document storage, the pay-off in our society also has escalated with a great increase in duplication and creation of any educational or property-related files by giving a certain amount of money[10]. These problems can be destroyed by using blockchain as a service for storing files. This will be a mechanism for easy recovery of documents, complete validation of data, and easy elevation of data as well. All of these systems will help us to greatly reduce trickery, bribes, and pilfering of documents.

2. Background

Document management currently, in this epoch, is done by storing it in a centralized DB system.In this centralized database system if a single change is made to the database, then every other person/office connecting to that database for getting information will get erroneous results. Also, there is expunging and overhauling of data in the centralized DB system[19], thus making the changed information irretrievable. Thus, the duplicates of documents and thefts can be easily done in the current epoch[11]. These problems are dealt with in our model by using a decentralized ledger system, instead of centralized databases.

The blockchain is a data structure that separates the data into containers - the blocks. The blocks are quite comparable to nodes in a linked list. Each block links to the previous block using a hash. A blockchain is made up of blocks that create a continuous chain. The end of the blockchain is always where fresh blocks are added [3], [4]. Transactions, among other things, are the most important aspects of the block chain. Hyper ledger and smart contract etc.

Each component is explained as:

1. Transaction:

The transaction is recorded in block chain as an asset or like a ownership and they are verified and accessed all over the nodes. These transactions are processed using timestamp as fig 1.

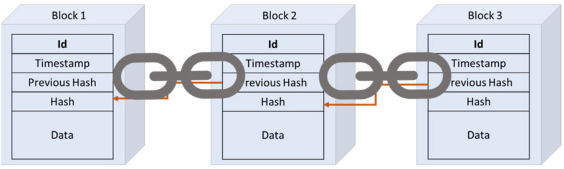


Fig.1. Time stamp

2.Peer network:

Block chain is a ledger which runs on a p2p network and is managed by a central server over the internet. As a result, they aren't vulnerable to a single point of failure or

Manuscript received June 5, 2022
Manuscript revised June 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.6.84

malware[15]. For the system to last longer, every member shares storage and computational energy.

3.Ledger system:
Ledgers are independent nodes to record, store and synchronize transactions in their respective e-ledgers.

4.Smart contract:
Smart contract are some application program which are saved on a block chain that runs on a certain user defined conditions they are written on solidity.

3. EXISTING SYSTEM

The authors of [2] presented a method for dividing medical files that used a limited shared data technique. Data packets should be restricted as separation data inside the doctor-patient context, as they could provide an unsecured site for theft to gain access to private medical reports for which the patient has opted to not even divulge specific information. If there are more partners inside the network, the writers agree that recognizing a patient to use a variety of techniques is likewise not a viable alternative for provisioning confidential material. The key information of a patient can be determined by combining ages, religion, region, day of enrollment, and medical issues[5] utilizing best fit consensus techniques. The author suggested a "ceremonious major data exchange consensus" [14] make data shareable among disparate organizations

.

4. PROPOSED SYSTEM

In this system,Fig 2 we are using ipfs for file storing the documents in a secure manner which is based on content addressing. In the case of files here, no copy of the file was created instead only an encrypted hash is provided to the recipient through which he can access the file. IPFS being content addressed helps in lowering the bandwidth expending and faster file ingress.

User can upload their personal files which are only accessible to certificates, important documents, etc.Using the decentralized system to store files provides the user with high reliability as our files are at risk from theft.Where anyone can post any type of document (pdf, image) to share with other users[16].Users can also plea a specific document by circulating a request.

We proposed to create an API in which the user can be able to upload the documents using meta mask gas price[12].When the user uploads a document it will generate transaction hash for the specific files and when it is shared the transaction hash of the sender and the user will be stored in the decentralized database.

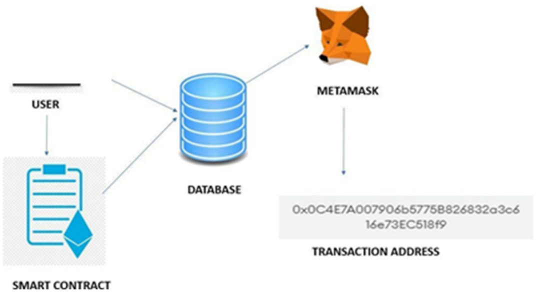


Fig.2. IPFS system

5. FILE UPLOAD

A file in .pdf,.jpeg format is uploaded by the end user. Regardless such files include unstructured data, in which they all follow the same pattern, which has been authorized by each person's internal regulatory authorities.

5.1 Smart contract

The uploaded file is then given to the smart contracts where the execution of the document is automated for the immediate outcome to reduce the time complexity[18]. This is then fed into data storage which contains plenty of versatile data which will generate in the form of hash.

5.2 Database

The database contains the document and the hash value of the respective file in that we use BigchainDB which is offering decentralization[7], immutable assets. . The data stored in the database is transformed into a 256 long bit hash function using the SHA-256 hash algorithm.

A hashing with such a range of 256 bits is known as SHA-256 (secure hash algorithm). It's a hash function for the power steering. A data is divided into 512 = 16 32 bit blocks, with each block requiring 64 successions. It will use this to set default values for the eight buffers.

a = 0x6a09e667

b = 0xbb67ae85

c = 0x3c6ef372

d = 0xa54ff53a

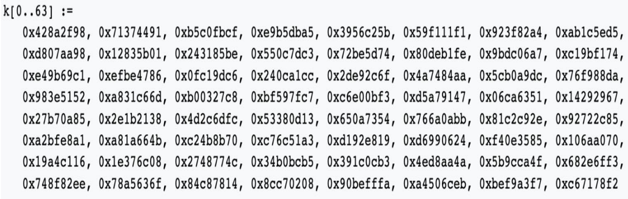
e = 0x510e527f

f = 0x9b05688c

g = 0x1f83d9ab

h = 0x5be0cd19

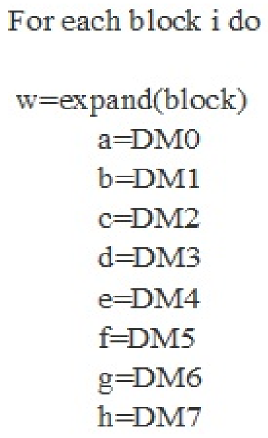
It is then store the key values in the form of arrayFrom k[0] to k[63] as shown in fig.3



```
k[0..63] :=
   0x428a2f98, 0x71374491, 0xb5c0fbcf, 0xe9b5dba5, 0x3956c25b, 0x59f111f1, 0x923f82a4, 0xab1c5ed5,
   0xd807aa98, 0x12835b01, 0x243185be, 0x550c7dc3, 0x72be5d74, 0x80deb1fe, 0x9bdc06a7, 0xc19bf174,
   0xe49b69c1, 0xefbe4786, 0x0fc19dc6, 0x240ca1cc, 0x2de92c6f, 0x4a7484aa, 0x5cb0a9dc, 0x76f988da,
   0x983e5152, 0xa831c66d, 0xb00327c8, 0xbf597fc7, 0xc6e00bf3, 0xd5a79147, 0x06ca6351, 0x14292967,
   0x27b70a85, 0x2e1b2138, 0x4d2c6dfc, 0x53380d13, 0x650a7354, 0x766a0abb, 0x81c2c92e, 0x92722c85,
   0xa2bfe8a1, 0xa81a664b, 0xc24b8b70, 0xc76c51a3, 0xd192e819, 0xd6990624, 0xf40e3585, 0x106aa070,
   0x19a4c116, 0x1e376c08, 0x2748774c, 0x34b0bcb5, 0x391c0cb3, 0x4ed8aa4a, 0x5b9cca4f, 0x682e6ff3,
   0x748f82ee, 0x78a5636f, 0x84c87814, 0x8cc70208, 0x90befffa, 0xa4506ceb, 0xbef9a3f7, 0xc67178f2
```

Fig.3 Key Values

The whole hash is divided up into 512-bit pieces It performs 64 rounds of operation on ever block, with the result of each block pattering a the input for another block[20]. The generated 256 bit hash function is then fed into metamask for the transaction as shown in fig.4.



```
For each block i do

 w=expand(block)
       a=DM0
       b=DM1
       c=DM2
       d=DM3
       e=DM4
       f=DM5
       g=DM6
       h=DM7
```

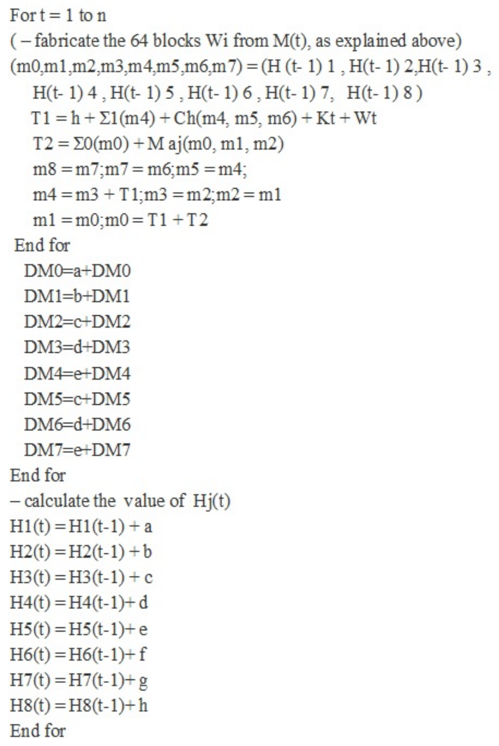
Fig. 4

5.3 Hash computation

First, 8 variables are their prime values and the first 32 bits of the fragmentary value of the square roots of the first 8 initial numbers:

H1(0) = 0x6a09e667
H2(0) = 0xbb67ae85
H3(0) = 0x3c6ef372
H4(0)= 0xa54ff53a
H5(0) = 0x510e527f
H6(0) = 0x9b05688c
H7(0) = 0x1f83d9ab
H8(0) = 0x5be0cd19

Next, the block as shown in fig.5 is executed only one at a time:



```
For t = 1 to n
( – fabricate the 64 blocks Wi from M(t), as explained above)
(m0,m1,m2,m3,m4,m5,m6,m7) = (H (t- 1) 1 , H(t- 1) 2,H(t- 1) 3 ,
   H(t- 1) 4 , H(t- 1) 5 , H(t- 1) 6 , H(t- 1) 7,  H(t- 1) 8 )
   T1 = h + Σ1(m4) + Ch(m4, m5, m6) + Kt + Wt
   T2 = Σ0(m0) + M aj(m0, m1, m2)
   m8 = m7;m7 = m6;m5 = m4;
   m4 = m3 + T1;m3 = m2;m2 = m1
   m1 = m0;m0 = T1 + T2
 End for
  DM0=a+DM0
  DM1=b+DM1
  DM2=c+DM2
  DM3=d+DM3
  DM4=e+DM4
  DM5=c+DM5
  DM6=d+DM6
  DM7=e+DM7
End for
– calculate the  value of  Hj(t)
H1(t) = H1(t-1) + a
H2(t) = H2(t-1) + b
H3(t) = H3(t-1) + c
H4(t) = H4(t-1)+ d
H5(t) = H5(t-1)+ e
H6(t) = H6(t-1)+ f
H7(t) = H7(t-1)+ g
H8(t) = H8(t-1)+ h
End for
```

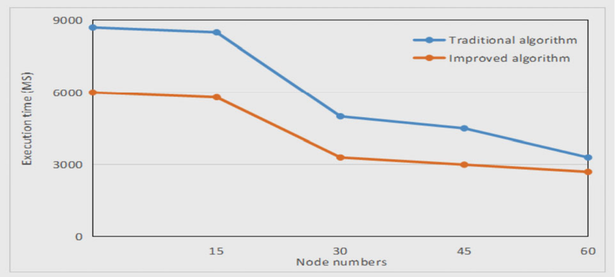
Fig. 5 Blocks of transactions

The hash of the message is the concatenation of the variables HN i after the last block has been Processed.

H=H1(N) ||H2(N) ||H3(N) ||H4(N) ||H5(N) ||H6||H7(N) ||H8(N)

VI. RESULTS

We have created a situation where the documents can be stored securely and the execution time for the existing system(Traditional algorithm) and the proposed system(Improved algorithm) varies as we use SHA256 algorithm. So that the scalability of the system increases by reducing the time taken. Fig.6 shows the result of the algorithm.



VII. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a blockchain-based document storage system that stores the documents, images, etc. In a form of hash which is then processed by the SHA-256 algorithm.

The proposed system does not have any analyzing mechanism to analyze what is written in the document. This information can be currently elucidated by a person. But in the future, the nodes can be made smart through Natural Language Processing and given the ability to understand one document from the forged one, thus raising a security awareness whenever it finds any theft in the currently received document.

References

[1] L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang, C. S. Hong, Edge-computing-enabled smart cities: A comprehensive survey, IEEE Internet of Things Journal 7 (10) (2020) 10200–10232.

[2] L. U. Khan, I. Yaqoob, M. Imran, Z. Han, C. S. Hong, 6G wireless systems: A vision, architectural elements, and future directions, IEEE Access 8 (2020) 147029–147044.

[3] K. Biswas, V. Muthukkumarasamy, Securing smart cities using blockchain technology, in: IEEE 18th International Conference on High Performance Computing and Communications, Syd- ney, Australia, 2016, pp. 1392–1393.

[4] Q. Feng, D. He, S. Zeadally, M. K. Khan, N. Kumar, A survey on privacy protection in blockchain system, Journal of Network and Computer Applications 126 (2019) 45 – 58.

[5]Bitcoin Market Capitalization, (accessed on 20 March 2020). URL https://coinmarketcap.com/currencies/bitcoin/

[6] D. C. Nguyen, P. N. Pathirana, M. Ding, A. Seneviratne, Blockchain for 5G and beyond networks: A state of the art survey, Journal of Network and Computer Applications 166 (2020) 102693.

[7] T. McGhin, K.-K. R. Choo, C. Z. Liu, D. He, Blockchain in healthcare applications: Research challenges and opportunities, Journal of Network and Computer Applications 135 (2019) 62 – 75.

[8] I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, Blockchain for healthcare data management: Opportunities, challenges, and future recommendations, Neural Computing and Applications (2021) 1–16.

[9] M. Razaghi, M. Finger, Smart governance for smart cities, Proceedings of the IEEE 106 (4) (2018) 680–689.

[10] Umer Majeed, Latif U. Khan, Ibrar Yaqoob, S. M. Ahsan Kazmi, Khaled Salah, Choong Seon Hong, Blockchain for IoT-based Smart Cities: Recent Advances, Requirements, and Future Challenges, Journal of Network and Computer Applications · February 2021,1-33.

[11] J. Yang, Y. Han, Y. Wang, B. Jiang, Z. Lv, H. Song, Optimization of real-time traffic network assignment based on IoT data using DBN and clustering model in smart city, Future Generation Computer Systems 108 (2020) 976 – 986.

[12] S. Musa, Smart cities-a road map for development, IEEE Po- tentials 37 (2) (2018) 19–23.

[13] E. Al Nuaimi, H. Al Neyadi, N. Mohamed, J. Al-Jaroodi, Ap- plications of big data to smart cities, Journal of Internet Ser- vices and Applications 6 (1) (2015) 25.

[14] Y. Yu, Y. Li, J. Tian, J. Liu, Blockchain-based solutions to security and privacy issues in the internet of things, IEEE Wire- less Communications 25 (6) (2018) 12–18.

[15] P. K. Sharma, J. H. Park, Blockchain based hybrid network architecture for the smart city, Future Generation Computer Systems 86 (2018) 650 – 655.

[16] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, C. Rong, A Com- prehensive Survey of Blockchain: From Theory to IoT Appli- cations and Beyond, IEEE Internet of Things Journal 6 (5) (2019) 8114–8154.

[17] B.Saravanan, V.Mohanraj, Dr.J.Senthilkumar "A fuzzy entropy technique for dimensionality reduction in recommender systems using deep learning" Soft Computing –Springer Vol. 23, No. 8, pp.2575-2583, April 2019

[18] G.Mohanraj,V Mohanraj, J Senthilkumar, Y Suresh," A hybrid deep learning model for predicting and targeting the less immunized area to improve childrens vaccination rate ", Intelligent Data Analysis 24(6):1385-1402,2020.

[19] Thiyaneswaran, B., Anguraj, K., Kumarganesh, S., Thangaraj, K." Early detection of melanoma images using gray level co-occurrence matrix features and machine learning techniques for effective clinical diagnosis", International Journal of Imaging Systems and Technology, 2021, 31(2), pp. 682–694.

[20] Chokkanathan K, Shanmugaraja P, Siva Shankar Ramasamy, Rujira Ouncharoen, Nopasit Chakpitak, "A survey on role of block chain in smart cities", International Journal of Computer Science and Network Security, Vol21, No.7, pp. 1-7.