Securing Educational Document Using Blockchain & IPFS

Rutuja D. Sanjekar[1]*, Dr. Balaji M. Patil[2]

***Corresponding Author: -** Rutuja D. Sanjekar
*1, 2 School of computer engineering & technology, MIT World PeaceUniversity Pune, Maharashtra, India

Abstract
The block chain is able to store shared and completely transparent information on an immutable ledger. As most crucial thing in an any industry is information. Success in industry is proportional to the speed at which it receives accurate information. So, the work of delivering fast and accurate information is done by Block chain technology. This ispossible because block chain is able to store shared and completely transparent information on an immutable ledger. Many cases of fake documents/certificates are encountered in educational system. As these cases are very high in number therefore it is totally unnoticed. So therefore, as a solution, blockchain based system can be used to store all the educational documents and certificates. Blockchain system is immutable and completely decentralized so no one can manipulate the data. Physical verification of user's document is very time consuming and tedious task. As this type of document verification system are centralized therefore, they are open to various intrusion attacks and also, they are not completely trustworthy for giving validation to particular user based on their educational history. In this paper, system illustrates blockchain base system in which students document can be stored and get verified on decentralized platform. At this moment also there are many organizations which conduct the process of document verification in traditional way like physical verification, etc. which is cannot be considered as best way of verification, thus blockchain based systemcan be opted as best solution to this. Many of the blockchain based systems are using IPFS for storage of data. But while using IPFS and blockchain together for storing data it is very important to ensure security. Hence, to protect the data over blockchain IPFS based system this research has proposed a novel approach by implementing visual cryptography and NTRU algorithm so that this will add extra layer of security to the data which is stored on this system.

Keywords: Blockchain, IPFS, Consensus algorithm, Smart contract.

DOI Number: 10.14704/nq.2022.20.9.NQ44373 **Neuro Quantology 2022; 20(9):3246-3251**

I. INTRODUCTION
The certificate is a document that can be considered as an evidence of qualifications, success, accountability for many events like student's learning ability, skills, etc. Certificate validation is a crucial part of hiring process. If any student is holding a forge document, then this will prevent from getting job. [1]However, the process of document validation is very time-consuming process which may lead to possibility of document getting forge.Therefore, it is essential to set up a reliable digital infrastructure for certificates. Blockchain is the latest technology which has features like transparency, security, reliability and traceability. As degree certificates hold very crucial information so they should not be easily accessible to anyone. Hence it is very important to design a system which is decentralized, transparent and trustable system that can verify the genuineness of document.[3] This blockchain based system should be able to verify the authenticity of documents. Hence this research has proposed a blockchain based system that can securely and safely store and validate the documents. In this research IPFS is used for off-chain storage.[4] IPFS is a type of storage system which can be used to store the documents directly on it instead of storing it on blockchain which helps the system become cost efficient. In Ethereum, blockchain will store the hash returned by IPFS.

The advantage of using this structure is that the data will be stored on IPFS and hash returned from IPFS is stored on blockchain so any change in IPFS data will result in change in hash which is stored on blockchain. Hence for the attacker it will be a tedious task to change the hash accordingly. But apart from this , in order to add extra layer of security this research is implementing visual cryptography, so that privacy concerns get eliminated.

These are the contributions made by this research work :

- Deployed a private Ethereum blockchain network. Designed a smart contract to store the data into IPFS and hash returned by IPFS stored in the Ethereum blockchain.
- Security of data stored over IPFS will be provided by implementing visual cryptography and NTRU algorithm.
- Carried out the performance analysis of IPFS and Implemented cryptography algorithm by considering parameters such as Key Generation Time, Share Generation Time, Encryption-Decryption of document, Data uploading and retrieval time based of file size.

The paper is structured as follows: Section 2, present structure of blockchain along with key elements of blockchain. Section 3 includes related works on securing educational documents using blockchain. In Section 4, included the proposed system using Ethereum and IPFS. In Section 5, the result section describes the performance of Ethereum blockchain. In Section 6, included conclusion and future work.

II. BLOCKCHAIN STRUCTURE

A. Block

A block is characterized as a data structure which is used for storage of information. The block comprises of block header and the block body. As there are so many blocks in blockchain then how will differentiate each block and so in order to create that chain and to differentiate each and every block it is important to have Block Header. Block header contains different elements like version, previous hash,timestamp, Merkle root.

B. Chain

In blockchain network, two blocks are connected to form a chain. The link between blocks is formed with the help of hash. Hashing algorithms like SHA1 or SHA2 are used to generate hash for the old block data. So, this chain is formed with the help of hash which helps to make the blockchain inaccessible.

C. Smart Contract

Ethereum is blockchain which contains the line of code, so if this code represents any kind of contract, then will call it as smart contract. When an event outlined in the smart contract is triggered then code executes automatically. For the implementation of smart contract solidity which is a high-level programming language is used. The smart contract process gets executed without need of third party. Because of smart contract manual effort of execution are reduced as they are automated with.

D. IPFS

IPFS (Interplanetary File System) is a peer-to-peer file storage system that contains different communication protocols. IPFS is used to store and share the data in distributed environment. In this global file system to identify each file uniquely IPFS uses content-addressing which means information stored on IPFS can be retrieved based on its content and not its location.

III.LITERATURE SURVEY

The utilization of physical copies of documents creates a large overhead in terms of manual verification, paper storage, incurring high cost and inconvenience. And there could be a breach of privacy and personal security as there is no control on access to the certificates. Hence, this research have come up with blockchain as a solutionto this problem.

Blockchain based document verification system was designed by [5], Jiin-Chiou Cheng, et.al authors. They discuss that blockchain based system in which hash value is calculated for digital copy of certificate and that hash value will be stored into blockchain. After that Blockchain stores QR code and unique serial number generated for the document. Authenticity of certificate can be verified by mobile phone scanning or website enquiry. The method of certificate application and automatic certificate granting are open and transparent.

An android application which was used to provide secure verification of certificates was designed by A. Gayathiri, et.al [6], authors. This blockchain based system prevents the certificate forgery and uses chaotic algorithm for the purpose of generating the hash value for the certificate. Sampling and quantization are used to convert paper certificates into digital certificates. Registration of students and uploading their certificate these operations are performed by the admin. Verification of certificate can be done with verifier credentials. But storing documents on blockchain is not feasible at all for large size files.

Decentralized application was developed by Padmavati E. Gundgurti, et.al [2]: authors using blockchain in order to stop the forgery of certificates. Cryptography technique like SHA-128, SHA-256 are used by user to ensure high level of security, which in turn generates random key for hashing purpose. With the help of this system, it will be very easy to track the changes in the system because modification in the file will result into key change. So, in this way high level of security is provided to user's certificate.

Traditional X.509 public key infrastructures was explained by Ze Wang, et.al [8] in which Certificate Authoritysigns certificate and then it is validation is performed in SSL/TLS network. Certificate Authority can ensure thehigh level of security as this infrastructure can also avoid signing of dishonest authentications. This system introduces reasonable overheads in terms of storage, certificate validation delay, communication, and incentivecost.

Instead of storing documents into blockchain network, Pavitra Haveri, et.al [1] authors suggested to store documents into IPFS network. And after that generated hash is stored on blockchain network. Validation process is performed by comparing hash provided by user and hash stored on block chain. In this way efficient way of document verification is provided by this system.

Gunit Malik, et.al [4] authors also discuss the approach to store documents in IPFS. They developed system which is based on private permissioned blockchain for verifying the documents. With introduction of this system which is based on private permissioned blockchain it reduces time taken for document verification andalso it has been 19 achieved low failure rate. Access control policy need to be implemented to enhance privacyof user details.

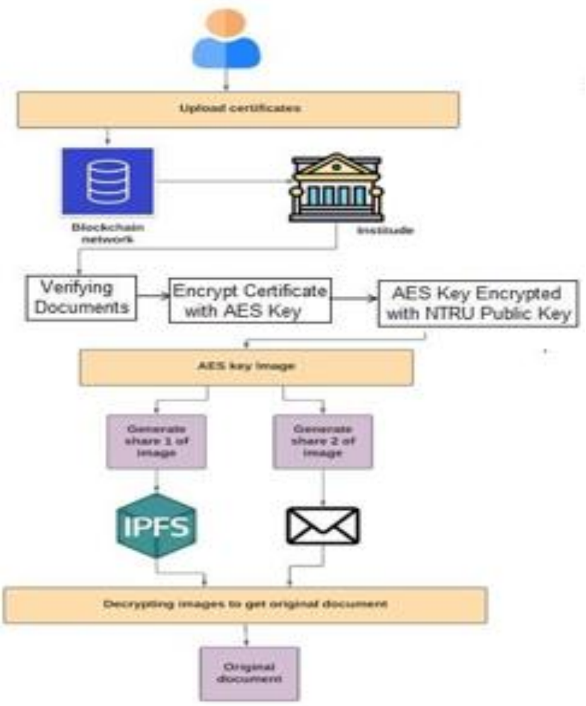
Different area of educational system that can be implemented with blockchain application are discussed by Ajay Kumar Shrivastava, et.al [7] authors. They proposed a blockchain based system which is developed in order to solve the problem of education system. In this system to appreciate the student's work crypto currencies are given to them. In this work, it showcases the different application of blockchain in education system and also addressed that how it will solve the problem in existing education system. In this system, as the number of transactions is more therefore it is very difficult to do perfect assessment and the performance of system will get affected as number of transaction increases. Some authors discuss the approaches where hardcopy of document is secured using blockchain and techniques like OCR are used in thisblockchain based system.

Saqib Rasool, et.al [3]: discuss about document verification system, in which blockcerts limitations are handled with the introduction of docschain concept. With the help of Docschain concept, document verification system becomes more efficient and, in this system, it is using OCR techniques document which are in hardcopy format. But transaction time for storing data on block chain and network is much more.

Ahmed Badr, et.al [11] authors also developed system in which hardcopy of document is used. So in order to validate the hardcopy documents in blockchain environment different technologies were implemented like 2D barcodes, OCR, cryptographic hashing. This system was developed for verification of hardcopy documents and in order to achieve the integrity, but the techniques used in system are very expensive. Forgery detection and integrity assurance was achieved by using the expensive techniques and in this system paperless environment was fully not achieved. The drawback of the system is that it is only directed towards academic institutes. Other organizations and industries are not included.

IV. SYSTEM OVERVIEW

Blockchain and smart contract based a decentralized authenticated application can be developed in order to stop the forgery of certificates. The information stored in this blockchain system is inaccessible which means the information cannot be manipulated. Even if a stranger or hacker tries to access or manipulate theinformation then the hash value of block chain gets replaced. So, for this the hacker has to again find the hash for the all the blocks in network, which is rarely achievable. Thus, blockchain provides high level security for storage of documents. Blockchain based document verification system is highly reliable as blockchain are replicated across all the nodes of network. In case of larger data storage, it is beneficial to incorporate the IPFSfeatures along with this blockchain and smart contract features. Such system helps to avoid the forgery of document, ensure the authenticity and also speedup the document verification process. Fig 4.1 shows the proposed architecture diagram of Certificate Validation System.



The above Figure 1 shows secured storage of certificates in distributed blockchain environment. In the first part students upload the certificate. Then uploaded certificate encrypted with AES key. And AES key will be encrypted with NTRU public key. Then using concept of visual cryptography will create encrypted AES key image and divide into 2 shares. One share of image stored on IPFS and other will be provided to student which is sent over mail. Admin will play role for the document verification.

Algorithm Implemented: -

NTRU Algorithm: It is difficult to deploy mobile java security in mass market mobile devices primarily due to size and speed constraints. NTRU, a relatively new public key crypto-system is based on the shortest vector problem in a lattice, and comes with many advantages as compared with other cryptosystems, such as high speed and low memory use that provides the possibility to overcome the constraints. NTRU cryptosystem uses two approaches to optimize the algorithm, such as changing forms and using low hamming weight products. The changing form approach simplifies both the key generation and the decryption, and the use of low hamming weight products increases the speed of the convolution multiplication by nearly 2 times. Experiments on the performance of enhanced NTRU-251 systems shows that NTRU has advantages over RSA,DES. For a similar security level, the key size of NTRU is less than a quarter of that of RSA. Apart from this, the speed of NTRU is faster than that of RSA. Also, the key generation is approximately 200 times faster and the encryption is almost 3 times faster while the decryption is about 30 times faster. So, in this research they have deploy NTRU algorithm in place of RSA, DES thus saving time and energy along with increased security.

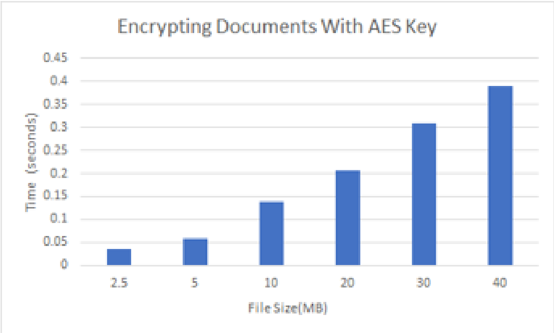
Visual Cryptography: Visual Cryptography is a technique of encryption which is used to hide visual information in a way that it can be decrypted by the human visual system, without using any decryption algorithm. By superimposing shares, the secret of visual cryptography can be reconstructed visually. When thedata is hidden within multiple images (known as shares), it is completely unidentifiable. While the shares are separate, the data is completely unclear. Each image holds different pieces of the data and when they are brought together, the information can be recovered easily. All the shares rely on one another in order to obtainthe decrypted information. There is hardly any way that anyone could decode the information contained within any of the shares. When the shares are brought together, decoding is possible as they get overlapped on one another. At this point, the data becomes instantly available. No computerized algorithm is required at all in order to decrypt the information. With the help of human visual system (HVS),all decryption process is performed, which is also referred to as a secret sharing problem.

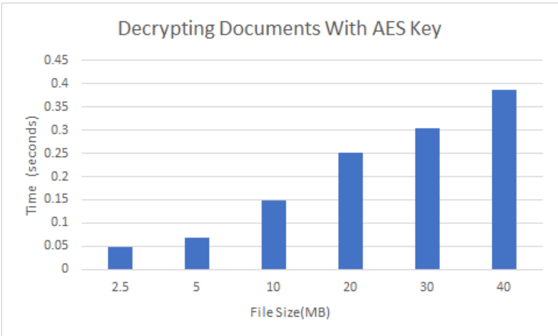
V. RESULTS AND DISCUSSION

Ganache is a personal blockchain that enables the building of distributed application, it allows to develop, deploy and test the dApps in secured environment. Smart contracts are developed and deploy on remix software. With the help of remix software, it can connect to remote node like Ethereum client. The details of system configuration are shown in Table 1.

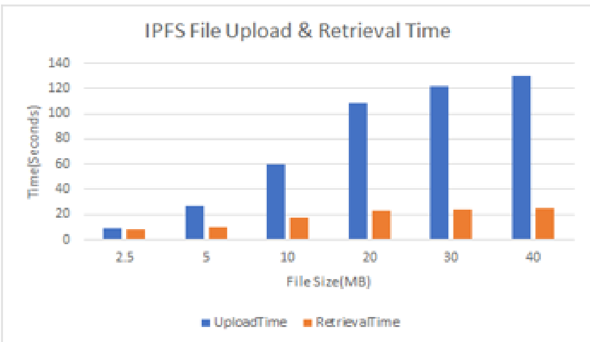
Component	Software	Version
Operating System	Windows	10
Blockchain	Ethereum	ETH
Blockchain Interface	Ganache	v2.5.4
Smart Contract	Remix	0.24.1

The graph (a) & (b) shows the time taken for encrypting and decrypting documents with AES Key.





We have experimented with 2.5,5,10,20,30&40 MB size files. We observe that with the increase size of file, time required for encryption increase, same is the case for the decryption of file with AES Key. Therefore, file size is proportional to the time taken for encryption-decryption process with AES Key.



In another test case we analyse the proposed model by measuring performance of IPFS System. The experiment with IPFS involves uploading files with varying file sizes, ranging from 2.5,5,10,20,30&40 MB. We perform this experiment with the aim to test the discrepancy in time taken to upload and retrieve files from the IPFS. We can see that uploading time is more than the retrieval time. As data uploading is one time process,and data retrieval process is more frequent. So IPFS will not be considered as problem for storage and retrievalof document.

Conclusion and Future Work

Blockchain Technology is most trading technology and it is adopted by many organizations. In Today's educational system, the process of validating document is not transparent and also very time-consuming process. Blockchain, IPFS based system has provided a way to securely store and validate the document in efficient way.Blockchain based system can provide the various security features like authentication, confidentiality, privacy and authorization of document, such system is beneficial for students, colleges and organizations also. It is advised not to store images on the blockchain due to high gas cost involved for each transaction. If 1KB of transaction data stored on blockchain, then it took 753,072 gas which is 0.03765 ETH. Calling the contract without adding any data will cost up to 0.003 ETH which is near around ($0.076) per KB, or around $76,000 USD per GB of storage. As data stored on blockchain network is costly, so in this research they are using IPFS as off-chain storage systemin which validated document will be stored. In order to ensure the security to this system, this research hasimplemented visual cryptography and NTRU algorithm. This system provides solution to the problem of document storage and security issue. In future we can implement the custom blockchain in order to ensure the effectiveness of how existing blockchains like Ethereum provides significance over the custom blockchain.

REFERENCES

Pavitra Haveri; U.B. Rashmi; D.G. Narayan; K. Nagaratna; K. Shivaraj "Securing Educational Documents using Blockchain Technology", 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)-2020.

Padmavati E. Gundgurti; Kranthi Alluri; Poornima E Gundgurti; Sai Harika "Smart and Secure Certificate Validation System through Blockchain ", Second International Conference on Inventive Research in Computing Applications(ICIRCA)-2020.

Saqib Rasool; Afshan Saleem; Muddesar Iqbal; Tasos Dagiuklas; Shahid Mumtaz " Blockchain-Based IoT Solution for Verification of Degree Documents ", 2017

IEEE Transactions on Computational Social System journal.

Gunit Malik; Kshitij Parasrampuria; Sai Prasanth Reddy; Seema Shah "Blockchain Based Identity Verification Model", 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN).

Jiin-Chiou Cheng; Narn-Yih Lee; Chien Chi; Yi-Hua Chen "Blockchain and Smart Contract for Digital Certificate ", 2018 IEEE International Conference on Applied System Invention (ICASI).

A. Gayathiri; J. Jayachitra; S. Matilda, "Certificate validation using blockchain", 2020 7th International Conference on Smart Structures and Systems (ICSSS).

Ajay Kumar Shrivastava; Chetan Vashistth; Akash Rajak; Arun Kumar Tripathi, "A Decentralized Way to Store and Authenticate Educational 22 ` Documents on Private Blockchain ", 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT).

Ze Wang; Jingqiang Lin; Quanwei Cai; Qiongxiao Wang; Daren Zha; Jiwu Jing , "Blockchain-Based Certificate transparency and revocation transparency", IEEE Transactions on Dependable and Secure Computing Journal.

Guang Chen, Bing Xu, Manli Lu & Nian-Shing Chen "Exploring blockchain technology and its potential applications foreducation".

Qin Liu; Qingchen Guan; Xiaowen Yang; Hongming Zhu; Gill Green," Education-Industry Cooperative System Based on Blockchain", 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN).

Ahmed Badr; Laura Rafferty; Qusay H. Mahmoud; Khalid Elgazzar, "A Permissioned Blockchain-Based System for Verification of Academic Records ", 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS).

D S V Madala; Mahabir Prasad Jhanwar; Anupam Chattopadhyay, "Certificate Transparency Using Blockchain ", 2018 IEEE International Conference on Data Mining Workshops (ICDMW).

Sthembile Mthethwa; Nelisiwe Dlamini; Graham Barbour "Proposing a Blockchain-based Solution to Verify the Integrity of Hardcopy Documents", 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC).

Raghav; Nitish Andola; Rakhi Verma; S. Venkatesan; Shekhar Verma, "Tamper-Proof Certificate Management System ", 2019 IEEE Conference on Information and Communication Technology.

Fernando Vidal; Feliz Gouveia; Christophe Soares "Analysis of Blockchain Technology for Higher Education, 2019 International Conference on CyberEnabled Distributed Computing and Knowledge Discovery (CyberC).

R. Poorni; M. Lakshmanan; S. Bhuvaneswari" A Secured Digital Certificate Application using Blockchain through Smart Contracts", 2019 International Conference on Communication and Electronics Systems (ICCES).

Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang,"An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" IEEE International Conference on Services Economics