SECURE STORAGE FOR SMART EDUCATIONAL INSTITUTION USING BLOCKCHAIN TECHNOLOGY

D. Sophia Navis Mary, Research Scholar [PT], Dr. S. Gopinathan, Professor,

Dept. of Computer Science, University of Madras, Chennai, Tamil Nadu

sophianavis@gmail.com, gnathan2002@gmail.com

ABSTRACT

Educational institutions have seen significant growth over the years, the use of innovative new pedagogy, secure storage, and global access of documents is important and on-demand in today's blended learning environment. Blockchain has created a huge potential in several industries by providing seamless, time-efficient, and secure transactions. In this paper, we propose a blockchain-based smart storage system to manage student's certificates, e-resources, academic credentials, and achievements rendering secure global access. The files are stored using the Proof of Work (POW) concept of Blockchain and access rights are defined using smart contracts. Also, this paper suggests how a public blockchain can be utilized to connect all the educational institutions under a university to provide global access, storage of educational records.

Keywords: Public Block chain, Proof of Work, educational records, smart contracts

INTRODUCTION

The Digital India movement aims to empower the country digitally by enhancing the infrastructure and the high-speed internet connectivity ensures that the government services reach every citizen. This movement makes various services available to everyone 24*7. Big data technology makes data collection, data storing, data analysis, and data sharing and feasible for the world. Cloud computing and IoT though provide many advantages, the major concern is security. To achieve information integrity, confidentiality, and securely share the government sector data various approaches are followed by the data owners. In the cloud storage approach, the centralized server is vulnerable to internal unauthorized physical access and external cloud storage attacks.

The digital signature was used for securing the privacy of the data owner information's. A digital signature is nothing but a cryptographic output of the sender data or embedding digital data to the user input data to convey that the data refers to a respective data owner. Usually, digital signatures are used to keep the receiver in a trustable zone making it feel that the message transmission is performed by the verified sender. Digital signatures, watermarking, handwritten signatures, stamped seals are used for protecting the user data and their privacy. E-mails, e-contracts, income tax submissions are examples of digital signatures in day-to-day life. Digital signatures use cryptographic primitives through the usage of the private and public keys during creation and its validation.

In traditional digital signature-based applications, the private key would be with the data owner as a file, an external device that has to be kept secure. Also, during access, the public key should be provided by the respective user which would be compared and validated. The complete authorization fails if anyone's validation is not satisfied [2].

However, the integration of these technologies in the educational sector is still in progress and these technologies are adopted by institutions at the training level only [3]. The adaptability of the technology in storing sensitive data, till now the records are maintained manually

BLOCKCHAIN TECHNOLOGY OVERVIEW:

Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the "chain," in a network connected through peer-to-peer nodes. Blockchain technology contains various elements including hash function, distributed ledger, P2P network miner, and consensus protocol.

Hash Functions: Blockchain uses a Hash function to generate a hash for the transaction which is referred any read/ write or update operation.

Distributed ledger: It is a shared and distributed ledger recording the transactions that happened in the chain.

Miner: The miner is responsible to validate the transactions and allow the genuine user to add a block.

P2Pnetwork: This network allows the users to share the data and update the information.

Consensus protocol: the agreement of individuals in the group to get access rights to share the data.

To achieve smart educational institutions, student's details, student's performance, student's marks, class-wise study materials, are the most important factors to transform digitally with security. In the existing system, the student details, marks, performance, study materials are physically managed either in the local educational server or third-party cloud server in which data tampering is possible. Each educational institution i.e., schools, colleges in the existing system are not integrated into a common platform providing transparency with access control, validating the student performance for scholarships, work, and during admission by other educational institutions and internship is a complex task.

Integration of blockchain technology into our existing education system provides global access to quality study materials among the students across the state with secure transmission providing privacy and authenticity. During pandemic like covid19, where traditional classroom-based education is a challenge, blockchain-based student details maintenance, marks accessing study materials can be achieved using Proof of work (Digital Signature generation using merle tree), Smart Contracts (Privacy-Preserving), and hyper ledgers (Transparency among the blockchain network).

2. RELATED WORKS:

[4] In this article, El-Gamal digital signature is been discussed in which the authors proposed asymmetric based approach with discrete logarithm issue. El-Gamal signatures invoke pair of keys such as public and private keys. The disadvantage of this digital signature generation approach using El-Gamal is time-consuming and the ciphertext generated is twice the plaintext length [5].

[6] This research paper briefs RSA-based digital signature generation. RSA algorithm is an asymmetric algorithm using both public and private keys which are used for encryption and authentication. There are several research papers proposing RSA-based digital signature generation because of its complex mathematics making the user data secure and difficult to crack. But the drawback of RSA based digital generation approach is the sender system becomes slow when large-sized data is provided for encryption. A third party is always required for validating the reliability of the public keys. Finally, if the intruder can able to compromise the system if he/she could tamper with the public key thus making RSA-based digital signature security a challenge [7].

[8] In this research paper, the Elliptic curve digital signature algorithm is explained. This algorithm invokes three phases namely key generation, generation of signature, and validation of signature. ECDSA is a recent encryption technique that is based on elliptic curve logarithmic issues. Though it is one of the secure digital signatures, figuring the exact curve during the setup phase is more complex. Also, ECDSA got some disadvantages like the generation of key and encryption time performance is slow. In ECDSA algorithm breaks when the sender message length is greater than the bit length [9].

[10] This research paper briefs how blockchain can be adopted in the health sector. To their knowledge, this was the first research approach for applying blockchain technology to the heath

sector. However, this paper significantly explains theoretically the functionality and the proposed architecture advantages.

[11] This paper explains the integration of blockchain in the health and biomedical sector. It explains the concepts involved in blockchain technology. This paper extends how traditional practices in medical data management, processing of insurance for patients, researches in the medical field, and manual ledger work of patient personal and medical data can be automated in a secure manner by introducing blockchain technology. This paper does not address the technical and experimental approaches.

[12] This paper, explains how blockchain can be used for maintaining student's personal and academic records. In this IMS comprehensive learner record all the student's certificates, degrees, personal and co-curricular skills, academic performance, courses are stored in the digital form. But this paper uses the decentralized-based approach for storing the data protection from internal and external intrusion.

[13] This paper proposes new ideas of how blockchain technology can be used by educational institutions. Various aspects like student recognition, academic internal performance, rewarding best performance, student certificates storage, student funding can be automated, stored, and transmitted securely invoking blockchain technology.

3. PROPOSED METHODOLOGY:

In the educational sector, several gaps are identified and challenges in the current system like rural students registered under the same board of studies won't have an opportunity to access study materials or learning content which urban students registered under the same board does have when students migrate from existing institution to a new one, the progress record of the respective student is disconnected as the progress record are maintained within the institution server and not being on a common server which can provide global access to analyze the performance and progress of the kid, the current institutions under a common university don't have a platform with sufficient data to analyze students personal skills, learning adaption skills, extra-curricular skills before admission enrolment and Student and study materials are stored in a centralized server which is vulnerable to attacks.

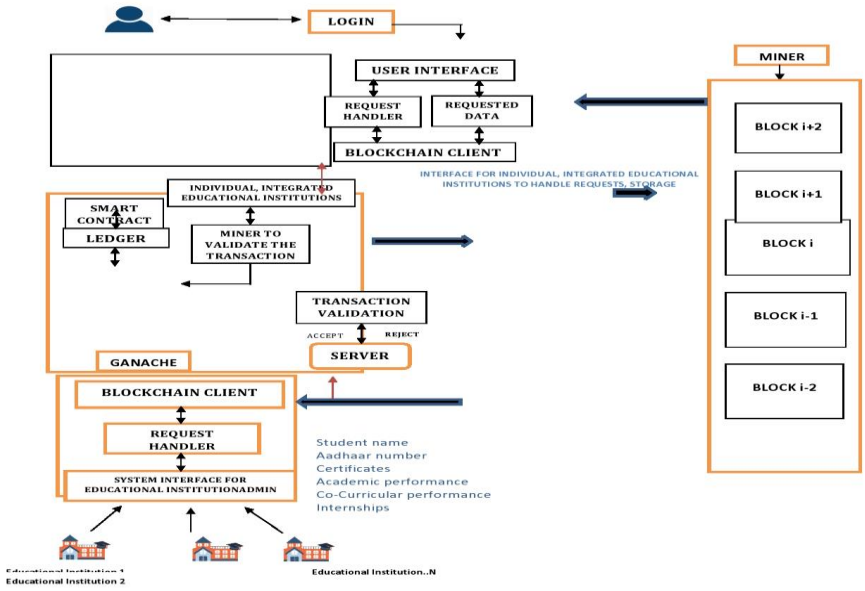


Fig 1. System Architecture of Storage

3.1 BLOCKCHAIN-BASED SMART STORAGE:

In this paper, we propose a smart and secure educational data store that allows global access by integrating all students within a common public network using blockchain technology.

In the proposed architecture Fig 1, only authorized individuals would be able to authenticate and upload certificates, study materials, academic performance, and achievements to the blockchain network using their private key like university registration number. On another hand, using the respective student number other educational institutions, organizations can able to request access. The upload of items would be validated by miners within the blockchain network and after successful validation; a new block is created and indexed to the ledger.

In this architecture, only authorized individuals would be able to upload the documents to the blockchain network using their private key like university registration number. On another hand, using the respective student aadhar number of other educational institutions, organizations can able to request access. The upload of items would be validated by miners within the blockchain network and after successful validation; a new block is created and indexed to the ledger.

Algorithm 1: Add a new block in chain

Add Block (stuid,staffid,adminid,adharno, data block)

//**Input:** A request from a client, unique id of user, data block

// user id may from student, staff, admin Bn- existing Block, Cn-n th block in the chain,

Db- data block to be added. Pk public key

//**Output**: A new block is added into the chain

```
While(true) do
 if( stuid is valid) then
      Add-student(Bn,Cn,Db)  //Add-student to the blockchain network
      Grand-access(Cn,Db,Pk)
      else
         Doesnotexist(Cn)
       end  if
 if( staffid is valid) then
   Add-staff(Bn,Sn,Db) //Add-staff to the blockchain network
  Grand-access(Sn,Db,Pk)
else
Doesnotexist(Sn)
 end if
If( adminid is valid) then
Add-admin(Bn,An,Db)//Add-admin to the blockchain network.
Grand-access(An,Db,Pk)
 else Doesnotexist(An)
 end if
end while
```

```
Int N:( 0 means suspect, 1 means genuine user)
For all (N) do
If behavior node(N) then No Update(Cn,Sn,An)
Else
Remove update(cn,Sn,An)
End if
End for
```

Algorithm 2. Append the Block into chain
//Input :new valid data block from the genuine user
//Output: The Block is added into the chain of blocks
1: Define the Block
2: Initialize the Block with index,timestamp,data,previousHash
3: calculateHash(newBlock)
4: Mining the Block by set the difficulty
5: Define the blockchain and its methods
6: Begin
7: create GenesisBlock
8: getLatestBlock
9: add new Block
10: if Chainisvalid= true
11: Append the new Block
12: else
13: reject the new block
14: end if
15: end

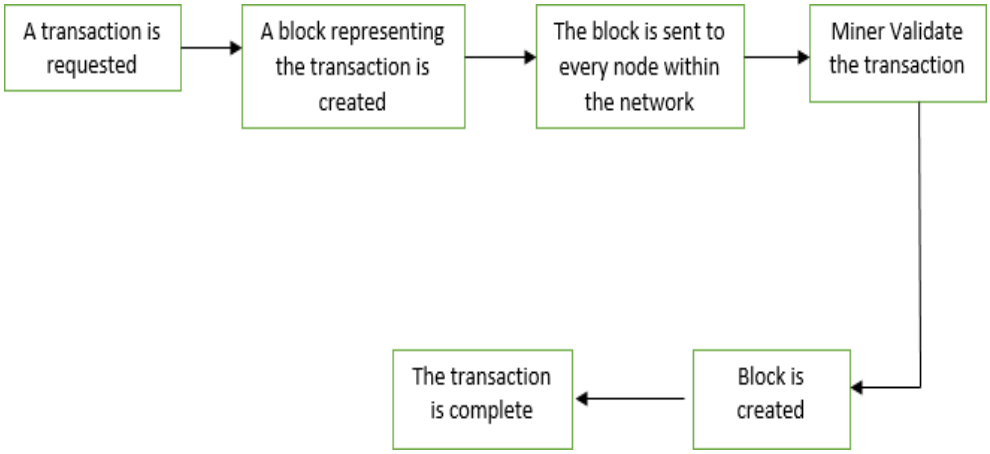
The proof of work validates the details and added assets with student details along with the time stamp in a block. A hash value would be created for a respective block along with appending the previous block hash value. The first block is called the genesis block. It doesn't have the previous hash value.

4.1 SMART CONTRACT CREATION:

A smart contract is an important element in blockchain technology. Smart contracts are used to preserve the privacy of the data owner. A smart contract is nothing but a set of predefined programs which would be validated during each transactional activity. It serves as a gateway to store information inside a chain. It contains the business logic of the application. It can validate or reject a transaction in the chain system.

4.2 HYPERLEDGER:

Hyperledger is a key aspect providing transparency and integrity among the students, educational institution representatives by providing a common ledger with preserving student sensitive information's. The students are identified with their unique university registration numbers. The ledger keeps updated after each successful transaction. The transactional requests and nodes are validated by miners associated with the network. The access restrictions and privacy-preserving can



be enhanced using hyper-ledger fabric 1.0. The transparency and monitoring within the educational institutions can be achieved using Hyperledger Fabric 1.0

5 .IMPLEMENTATION& RESULTS

In the proposed architecture, we used public blockchain for the experimental analysis. For public blockchain setup used Ganache, Metamask, for smart contracts used remix Ethereum, for application programming implementation use JavaScript. The ethers purchased by the data owners are kept safely in the Metamask wallet and during each transactional activities, gas value is been detected from the wallet.

First, the public blockchain environment is set with the help of Ganache server and the hash code value is generated for each user.

The data block of each valid user is generated and validated by the proof of work defined shown in Fig 3 before it is added to the blockchain. The miner in the network chooses the difficulty to validate the hashcode of each block. Ether is the transactional token that facilitates operations on the Ethereum network. To execute the programs and services in the Ethereum network require computing power in terms of Ether.

5.1 MetaMask Chrome Extension

MetaMask acts both as an Ethereum browser and a wallet. It allows users to interact with smart contracts and distributed apps on the web and create a wallet and submit Ether.

5.2 SMART CONTRACT EXECUTION

A smart contract is a program executed automatically, which consists of terms of agreement between two parties using the blockchain network . For simulation we use Remix IDE for writing smart contracts.

Deploy the smart contract at the Ethereum test network .After the transaction commits successfully, the address of the smart contract be visible. At first, all the transaction taken will be stored in the wallet of the user who is deploying the smart contract.

The time taken to create a new block in a block chain is calculated by a block is verified by miners, solve the hash and for the current transaction creates another block. In the proof-of-work consensus mechanism, a reward is given for solving a block's hash and creating a new block.

5.3 COMPUTATION COST CALCULATION

Gas refers to the fee, or pricing value, required successfully conducting a transaction or executing a smart contract on the Ethereum platform. In the Ethereum Virtual Machine each computation happening in the EVM needs some amount of gas. The expenses in small fractions of the cryptocurrency ether (ETH) , commonly referred to as Gwei. The cost of using this block chain technology is assessed in terms of Gas fees. In the Ethereum network the amount of transaction is measured in terms of gas price. The Ether spend for the transaction is defined as

Gas Fee/transaction= (∑ gas required to perform each operation in a transaction* gas limit.)

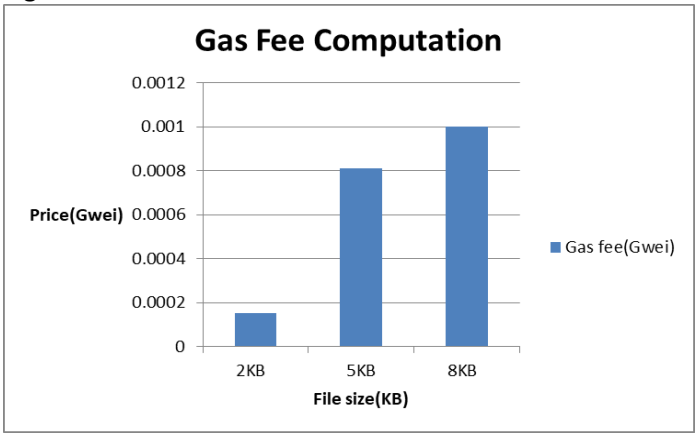
Gas limit = Max Amount of gas to spend on a particular transaction.

Transaction fee = Total gas used*Gas Fee

File Size	Gas fee(Gwei)
2KB	0.000151
5KB	0.000811
8KB	0.001

Table 1. The Gas fee for transaction

Fig3



Blocks	Execution Time(sec)
1	0.43
10	0.45
100	0.46

Table 2 : Execution time for New Block

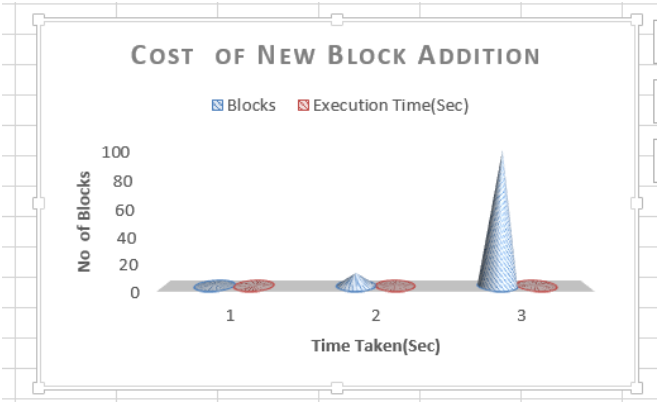


Fig 4: Cost of New Block addition in Block Chain

Table 2 gives the amount of gas detected from the wallet when a data blocks are added into the block chain which helps to understand the computation cost in this technology. Gwei is a cryptocurrency used in Ethereum network. the time taken to add a new block in a block chain in the network is computed in the simulation.

The paper implements the Block chain technology which use a merkle signature for securing the files. RSA and ECDSA and Merkle tree based signature are implemented for the analysis. The RSA based signature uses the private key and public key pair to validate the integrity of the data. In Table 3 show the time taken for generating signature for the data block using merkle signature, then the time for signature generation using Elliptic curve cryptography and well known RSA Signature.

FileSize (KB)	RSA (m/s)	ECDSA (m/s)	Merkle (m/s)
168	2.40	4.42	1.14
177	2.59	4.48	1.31
196	2.77	4.61	1.48
400	10	15	3

1500	27	33	15
2048	32	48	21
3000	40	78	29

Table 3. Comparison of Execution time to generate digital signature

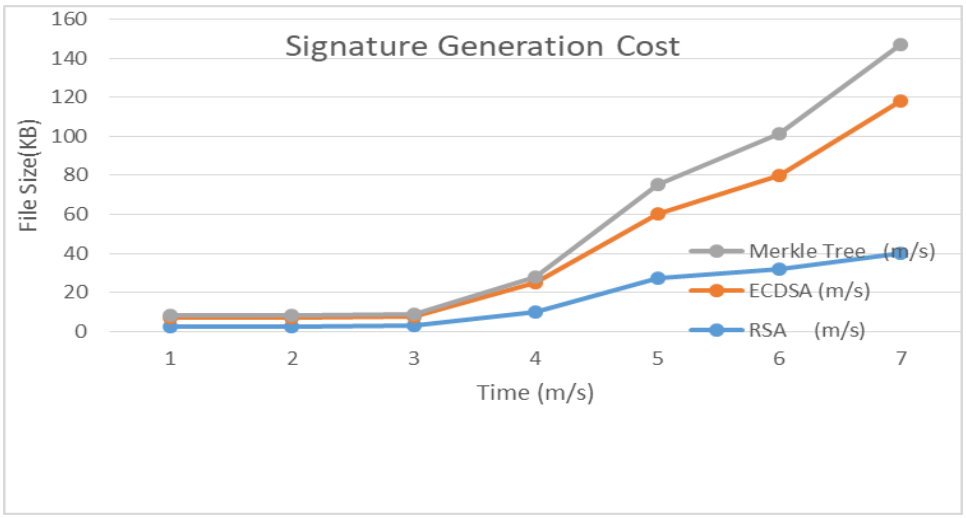


Fig 5. Comparison of signatures Generation time

6 CONCLUSION:

In this paper, we have proposed blockchain based secure framework for educational institutions and the e-resources available across several students. The major contribution of this paper is briefed how blockchain can be made adaptable for the current educational system for storage and maintenance of records. This system provides secure, efficient, better support for educational system information management. The student privacy is preserved using proof of work and smart contracts techniques used within the blockchain technology.

REFERENCES

[1] https://www.computerworld.com/article/3173616/the-sha1-hash-function-is-now-completely-unsafe.html

[2] http://www.e-mudhra.com/faq.html

[3] Siemens, G., & Long, P. (2011). Penetrating the fog: analytics in learning and education. EDUCAUSE Rev., 46(5), 30.

[4]www.inf.ed.ac.uk/teaching/courses/cs/ 1112/lecs/signatures-6up.pdf Date of access -22nd May (2012)

[5]ElGamal:Public-Key Cryptosystem Jaspreet Kaur Grewal,

[6]Cryptography and E-Commerce, A Wiley Tech Brief, Jon C. Graff, Wiley Computer Publishing, ISBN- 0471-40574-4.

[7] csrc.nist.gov/publications/fips/fips186-3/ fips_186-3.pdf Date of access -24th March (2012).

[8]www.ijcaonline.org/volume2/number2/ pxc387876.pdf Date of access -22nd May, (2012).

[9] Imem Ali, Comparison and Evaluation of digital signature schemes employed in NDN network Al, IJESA, Vol.5, No.2, June 2015

[10] Mettler M. Blockchain technology in healthcare: the revolution starts here. IEEE 18th International Conference on e-Health Networking, September 14–16, Piscataway, NJ: IEEE,

2016. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7749510 . Accessed March 3, 2017
[11] Mackey, T.K.; Kuo, T.T.; Gummadi, B.; Clauson, K.A.; Church, G.; Grishin, D.; Obbad, K.; Barkovich, R.; Palombini, M. 'Fit-for-purpose?'—Challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Med. 2019, 17, 68.
[12] Schmidt, P. (2016). Blockcerts–an open infrastructure for academic credentials on the blockchain.MLLearning (24/10/2016). Retrieved 2018-05-22, from https://medium.com/mit-media-lab/blockcerts-an-open-infrastructurefor-academic-credentials-on-the-blockchain-899a6b880b2f
[13] Grech, A., & Camilleri, A.F. (2017). Blockchain in education. Luxembourg: Publications Office of the European Union. IMS Global Learning Consortium (2017).Comprehensive learner record.https://www.imsglobal.org/activity/ comprehensive-learner-record.Accessed 28 May 2018.