EduBlocerts: Securing Institutional Data using Block-chain Technology

D. Durga Bhavani, D. Chaithanya

Abstract*: Educational Institutions are storing their data and their transactions in the physical media such as registers, books, records and in digital media like hard disks and in cloud storage. These type of storage media are insecure and are prone to data tampering. Even when they are protected with a password, they can be altered if the user's password has been hacked, which means the traditional methods of record keeping are insecure. Blockchain has a decentralized architecture which store and secure transactions transparently and there will be no central authority over those occurring transactions. So, a model is implemented which uses the core technology of the Block-chain to store and secure the institutional data which will be in the form of transactions. These transactions can be easily viewed by anyone in the connected network. Even if the data is tampered it can be detected easily. This model has the advantages of Block-chain minus the investments and risks associated with it.

Index Terms*: Block-chain, Consensus, Consortium, Data Tampering, Education, Institutional Data, Security.

I. INTRODUCTION

In any Educational Institution, the data and transactions are stored normally in paper and digital formats. These type of storage techniques are outdated in this current world because of the various threats arising day-by-day. No matter how we secure the data with passwords and firewalls they are still prone to tampering because of human's selfish needs. An Instructor or student can allegedly change their grades, alter the attendance and also create fake study certificates. These type of acts spoil the purpose of education and are everywhere degrading the quality of education. A Blockchain is a ledger without a central authority having control. It is an enabling technology for individual companies and institutions to collaborate with trust and transparency. It normally contains a growing list of publicly accessible records which are cryptographically secured from tampering [1].

So, a prototype model has been created and implemented which uses the underlying technology of Block-chain in a consortium type of network to store various types of institutional data in the form of blocks. This data can be viewed and accessed by anyone in the network, but they cannot modify it.

This particular model is not implemented on the real Block-chain but it uses its technology and is implemented within the institution. So only the participants of the network i.e., people of the institution can view and access the data without having to go through all of the formal procedures to obtain that data. So, this prototypical model is beneficial to the institution because it does not require cryptocurrency to store the data as the real Block-chain does.

A. Impact of EduBlocerts

In any institution records of all their transactions are stored in books, ledgers, and certificates. So, they can be accessed easily and is prone to data manipulation [2]. This is the main disadvantage of current record keeping formats. Not only losing the originality of the data there also exists a problem in storing those records. Storage of large sets of data and accessing them becomes a tedious task both in paper and digital format because the incoming data needs to be organized continuously and maintained securely.

This particular implementation of Block-chain in an Institution solves the following problems:

Data Manipulation: Since Block-chain is protected by Hashing that uses SHA-256 Algorithm it stores the data securely and makes it tamper proof.

Data Management: Blocks in the Block-chain are not a physical entity which deteriorates over time, they can be maintained easily.

Data Accessing: Block-chain has a centralized architecture so the data can be accessed without any formal procedures [5].

Therefore, a peer-to-peer record keeping system is implemented with the addition of cryptographical methods like digital signatures to ensure transparency, data security and easy storage of the records for educational institutions that will make sure no manipulation of data at any given point of time. Since digital signatures are created by hashing technique, the transactions which are created by the owner cannot be modified by third parties [5]. Thus, this prototype model uses a Consensus algorithm which is a fault tolerant mechanism and is used to achieve the necessary agreement on a single data value over a system where all the drawbacks of traditional methods of record keeping are overcome.

II. RELATED WORK

A. EduCTX: A Blockchain-Based Higher Education Credit Platform

EduCTX depends on the idea of the European Credit Transfer and Accumulation System (ECTS). It establishes a universally trusted, decentralized advanced education credit, and evaluating framework that can offer an internationally unified perspective for understudies and advanced education foundations (HEIs), just as for other potential partners, for example, organizations, establishments, and

Revised Manuscript Received on July 05, 2019

Dr. D. Durga Bhavani, Department of Computer Science and Engineering, CVR College of Engineering (Autonomous), Hyderabad, India.
D. Chaithanya, Department of Computer Science and Engineering, CVR College of Engineering (Autonomous), Hyderabad, India.

associations. EduCTX will process, oversee, and control ECTX tokens, which speak to credits that understudies gain for finished courses, for example, ECTS. HEIs are the companions of the blockchain organize. The stage is a first venture toward an increasingly straightforward and mechanically propelled type of advanced education frameworks. The EduCTX stage speaks to the premise of the EduCTX activity, which envisions that different HEIs would unite so as to make an all-inclusive efficient, simplified, and universal condition so as to dodge language and regulatory boundaries [3].

B. BLOCKCERTS: The Open standard for Blockchain Credentials

Blockcerts is an open standard for making, issuing, seeing, and checking blockchain-based certificates. These digital records are enrolled on a blockchain, cryptographically marked, carefully designed, and shareable. The objective is to empower a flood of advancement that enables people to have and share their very own official records [4].

III. MAIN MODULES AND PARTICIPANTS INVOLVED IN EDUBLOCERTS NETWORK

There are 6 working modules in EduBlocerts and they interact with each other by sharing the transactions and maintaining a consensus agreement [6]. They are: Attendance, Marks, Fee Management, Certificate Management, Personal details of Students and Faculty members. Here, Faculty takes attendance and gives marks to the students. Examination Branch issues course completion certificates. Administration department manages financial tasks like fee collection. Student takes care of his personal details and Faculty takes care of their personal details.

All the nodes in the network act as participants of the Blockchain [6]. Here in EduBlocerts, there will be four participants who communicate with each other as shown in Fig 1.

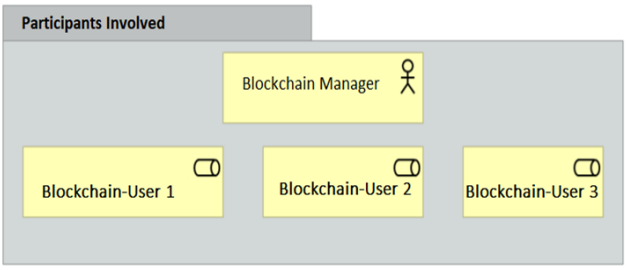

Fig. 1. Participants involved in Consortium Network

A. *Block-chain Manager (BM)*

Block-chain Manager is responsible for managing all the transactions, database services, and Block-chain services.

B. *Blockchain User 1: Administration Department*

It deals with the current activities of the Educational institution. It records the relevant information of all the current employees and students and guarantees the smooth execution of all the processes. In this model, we considered the processes like Managing financial transactions, storing personal information and crediting them. The educational institution develops student records that are indestructible and universal. This facilitates developing of a global standard of accreditation that will not need any verification thus eliminating the time to do such activities. If, in any case, a student loses his academic records, then he can get it from his home without going through the formal procedures at any given point of time.

C. *Blockchain User 2: Faculty*

The teaching staff verifies and stores their student particulars like attendance, assessment, behavior, leadership qualities and results obtained, etc.

D. *Blockchain User 3: Student*

The student is the pivoting participant in this model. He can always access his own records using a private key, but cannot modify the data. He can approach any organization for an internship, scholarship and employment without the barrier of country, language or time by providing his block's hash to the required person for his verification purposes [6].

IV. TRANSACTION MECHANISM

The Block-chain is a type of Distributed Network that follows a Consensus approach of single data value over a system. In a distributed network the transactions cannot be simply stored. They have to go through a step-by-step procedure of transaction mechanism [6]. It can be defined in five stages such as Transaction Encryption, Transaction Decryption, Block Creation, Block Authentication and Block Propagation as shown in Fig 2.

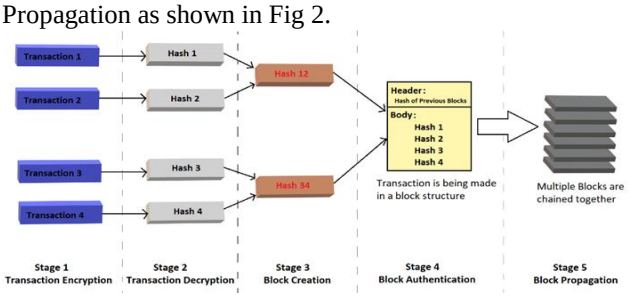

Fig. 2. Transaction Mechanism in EduBlocerts

A. *Transaction Encryption*

The data owner will initiate the transaction in which the details of the receiver's public key, the receiver's address and the transactional value is specified. After initiating this transaction, it will be encrypted with the sender's cryptographic digital signature, which authenticates the stored transactions.

B. *Transaction Decryption*

The signed transaction is sent to the network and received by all nodes of the network. Then the message will be validated by decrypting the digital signature. Further, it is sent to the pool of pending transactions where it waits till a block is created.

C. *Block Acknowledgement*

Any node in the network takes the initiation to create a block by combining with all other decrypted transactions which are in the waiting state. Once the block is created, it is broadcasted to each node in the network for authentication.

D. Block Authentication

The nodes, after receiving the block copies, start an interactive process to validate it and communicate with each other to check for single data value over a system. However, there might be a difference between Blockchain's branches when they do not share the same data value due to network issues. Therefore, it is necessary to reach a consensus on the block authenticity among all the nodes.

E. Block Propagation

Once a block is authenticated, it will be registered in the network as a verified block. Next block will be linked to the recently verified block. Further, these two blocks are formed as a chain and broadcasted over the network, where the future blocks will be propagated as a verified version of Block-chain [6].

V. IMPLEMENTATION OF EDUBLOCERTS

Since EduBlocerts is implemented in a consortium network with the assistance of blockchain technology, it pursues a similar working as the real blockchain and it doesn't require any type of crypto-currency like bitcoin to make the transactions.

Here, the functioning of Edublocerts is represented in the algorithm underneath. The procedure begins from Input information given by the participant to the final blockchain creation.

A. Algotithm

```
begin
  Step 1: for (i=1 to n)
          T=gets();
Step 2: En(T);
Step 3: De(T) = p(Wi);
Step 4: for (Wi = 1 to n)
    p(W1) + p(W2) + p(W3) +…+ p(Wn) = B[Wi];
Step 5: Hash {B[Wi]} = p(Ai);
Step 6: for (Ai = 1 to n)
p(A1) + p(A2 + Hash(A1))+ p(A3 + Hash(A2))+…
                …+ p(An + Hash(An-1)) = BC[T];
  goto: Step 1
end if T= null;
```

Abbreviations:

1. T = Raw form Data.
2. En (T) = Encryption of Raw Data using the Public key.
3. De (T) = Decryption of Encrypted data using the Private key.
4. W_i = Transaction ‘i’ in a waiting state where ‘i’= 1 to n.
5. p (W_i) = A pool of transactions which are in waiting state.
6. B [W_i] = Block containing n waited transactions where ‘i’=1 to n.
7. p (A_i) = Acknowledged Blocks in waiting state which are ready to be chained together. Here i represents the position of the block in the chain.
8. Hash { B [W_i] } = Hashing the block using SHA-256 Algorithm and storing it in BC[T].
9. BC [T] = Created Blockchain.

The User Interface takes the input from the user with the help of ‘gets ()’ command. Then the Raw Data will be encrypted using Public key and sent over the network. After the Encrypted Data has been received it will be now decrypted using the Private key and stored in a pool of waiting transactions.

In the next step, all the transactions in the waiting state are now grouped together into a block. Now, the block that holds some transactions will be hashed using SHA-256 Algorithm and the block will now be called as acknowledged block. This acknowledged block will now be stored in a separate pool of ready-to-be-chained blocks. All the Acknowledged blocks will now be chained together using the hashes of its previous blocks forming a Blockchain. This chain is propagated until the transactions are happening.

VI. RESULTS AND DISCUSSION

Each of the modules takes the input from the end user and stores the data in the form of blocks. These blocks are chained together propagating a chain. The data in these blocks are transparent and can be viewed by all other nodes who are participants in the network. Any node can view the data and transactions of all the nodes but those other nodes cannot modify those blocks. By this, the transactions will be transparent and tamper proof.

Consider a marks module which takes marks as input from the faculty and stores them on a blockchain as shown in Fig 3.

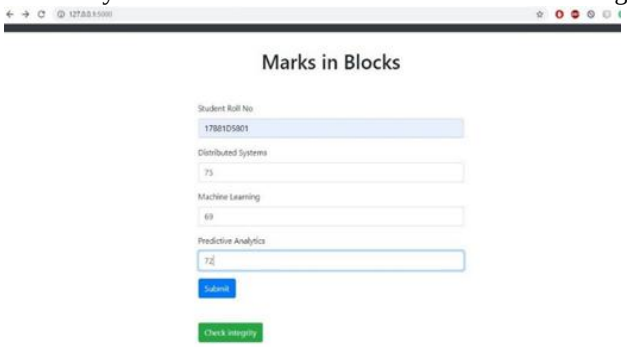

Fig. 3. Front-end of Marks Module

Now after we click on submit, those marks get stored in a blockchain form as shown in Fig 4.

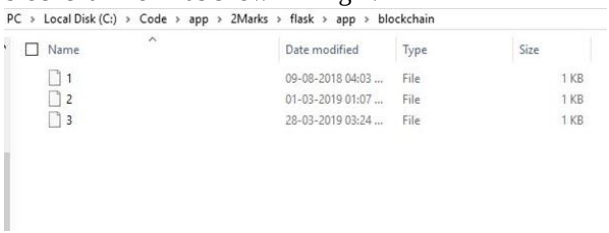

Fig. 4. Block Creation

These are the blocks in which transactions are stored and are linked together with hashes. This chaining process is continued until the transactions are going on. By this way, our blockchain is propagated.If a user wants to view the data, he can open that block directly and access the transaction as shown in Fig 5.

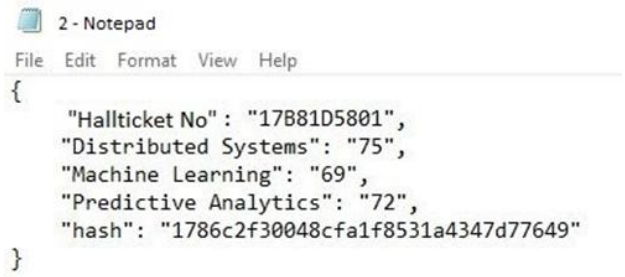

Fig. 5. Data Accessing

Even if the data is modified in the block by a third party as shown in Fig 6, it can be detected by checking its integrity from the front-end page as shown in Fig 7.

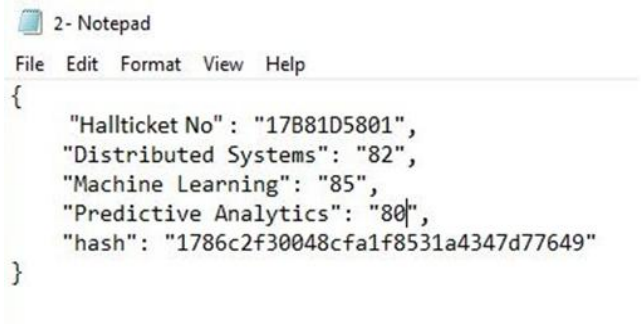

Fig. 6. Data is altered

Now the block that has been altered can be detected with its block number in the front end as shown in Fig 7.

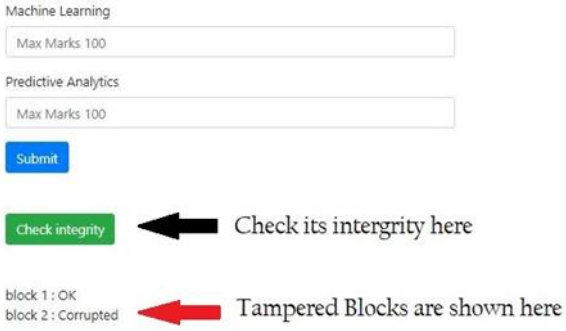

Fig. 7. Corrupted Block Detection

So, after the data tampering if we check its integrity, the tampered block with its block number will be shown as a corrupted block and the previous version of this altered block which is already distributed across the network helps in maintaining the consensus agreement and avoids the changes in the block. By this way, we can know if the data has been tampered by third party or not.

VII. CONCLUSION AND FUTURE WORK

Blockchain has a decentralized architecture and has the potential to revolutionize various industries besides educational sector. In this paper, a blockchain-based institution management system was implemented using smart contract which hashes every single transaction happening in the system, making them safe and secure even in case of data tampering. Each transaction of the modules which are connected together utilizing hashes, will be straightforward and can be seen by anybody in the network.

The transactions in this EduBlocerts can be created however can't be changed by anybody including the data owner as like a genuine blockchain, which guarantees that there is zero chance of information being altered. All the individual transactions of every module are broadcasted to all the active nodes in the network which means each module contains every transaction-hash pair of all nodes. When ever a new transaction has been added by the data owner it will also be broadcasted and chained to existing blocks in the network. Accordingly, this model especially takes care of the traditional issues of record keeping and their information security issues with the assistance of Blockchain technology. Since the represented model is an essential adaptation of how the institutional information and transactions are secured utilizing Blockchain technology, it may be additionally upgraded and refreshed with the required adjustments.

REFERENCES

1. "An overview of blockchain technology: Architecture, consensus, and future trends'' Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, in Proc. IEEE Int. Congr. Big Data (BigData Congr.), Jun. 2017, pp. 557–564. [Online]. Available: http://ieeexplore.ieee.org/document/8029379/
2. "Schools are using Blockchain: Blockchain goes to school" [Online]. Available: https://www.cognizant.com/whitepapers/blockchain-goes-to-school-codex3775.pdf
3. EduCTX: A Blockchain-Based Higher Education Credit Platform Available: https://ieeexplore.ieee.org/document/8247166
4. Blockcerts : The Open Standard for Blockchain Credentials Available: https://www.blockcerts.org/
5. "Blockchain Applications: A Hands-On Approach (2017)" Author: ArshdeepBahga, Available: "Blockchain Applications: A Hands-On Approach (2017)" Author: Arshdeep Bahga, Available: https://books.google.co.in/books?id=M7sanQAACAAJ&redir_esc=y&hl=en
6. "A Model for Securing Institutional Data using Blockchain Technology" Dr. D. Durga Bhavani, D. Chaithanya, in Proc. ICDECT-2019, 3rd International Conference on Data Engineering and Communication Technology, March 2019.

AUTHORS PROFILE

Dr. D. Durga Bhavani Professor, Department of CSE, CVR College of Engineering, India, has over 25 years of teaching experience for UG/PG students. She has published/presented high quality research papers in International Journals and proceedings of International/ National Conferences to support her research work. She is the life member of CSI, ISTE, and IAENG. Her areas of interest are Data Mining, Block Chain Technology, Cloud Computing, and Big Data.

D. Chaithanya PG Student, Department of CSE, CVR College of Engineering, India. His areas of interest are Distributed Computing, Block Chain Technology, Cloud Computing, and Internet of Things.