iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52379

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Educational Record Authentication Using Decentralized Consortium Blockchain Technology

Deep H. Bawane[1], Yogesh S. Sudke[2], Prof. Yogita N. Pore[3]
[1, 2]*Final Year Students,* [3]*Asst. Professor, Computer Engineering Department, Zeal College of Engineering and Research, Pune – 411041, Maharashtra, India*

Abstract: ***The current facilities provided by educational institutes across the global to authenticate educational records use centralized approach of maintaining a server. This introduces two key challenges. One is to provide sharing and browsing facilities even when there is server maintenance. The other is to prove the authenticity of the records. The first challenge may be resolved using cloud-based techniques. To address the second challenge, we propose a consortium blockchain based solution. By using off-chain storage for record update and management, third party modification to any valuable data can be known. The nodes in the decentralized peer-to-peer network are servers handled by recognized educational institutes which may be autonomous or affiliated. Using cryptography, the hash information of records is stored on a decentralized blockchain. This enables a student or a third party to quickly verify his/her marks by verifying hashes of them from a reputed peer-to-peer network.***

Keywords: Consortium Blockchain, Decentralization, RabbitMQ, Flask

I. INTRODUCTION

In the past few years digitalization has been highly emphasized in education sector. This is can be seen in the forms of online exams, online exam proctoring, and most importantly online results. Compared with the traditional paper physical records, digital records are stored on the storage medium which has a high degree of variability; hence such records could be easily modified during the processes of storage, transmission, and sharing [1]. Educational records are important for academic as well as professional opportunities. This makes the authenticity of these records a great topic along with their storage. Validation from a reputed network of institutions can be used as a way of proving authenticity. This can be achieved by using an immutable decentralized ledger maintained by multiple legitimate institutions.

A. Existing Mechanisms

Most existing methods to verify the records are provided by the issuing authority itself. A central server provides a digitally signed certificate which may or may not be accepted by a concerned party. Digi Locker is a service provided by the Indian government where only genuine digital documents can be stored which is a little more reliable. However, reflection of these certificates takes much time. During server maintenance or downtime all services are at halt. However, depending upon the nature of institution this service may not be available at all, i.e., traditional method of providing a physical copy. The downside of this is if the physical records are lost by human mistake, then complicated procedures have to be followed to reissue them.

B. Objective of this paper

The main motive of our project is to provide a fast and simple method to prove the genuineness of educational results without depending on the availability of the issuing authority's server. Another motive is to lessen the significance of carrying physical copies of the records. By maintaining a decentralized ledger, the network intends to nullify the effects of any wanted or unwanted modifications which made on existing records in the off-chain storage. This tries to eliminate the dependency on the issuing authority when it comes to authenticity of an educational record, as the maintained blockchain is capable of doing so without involvement of off-chain storage.

II. METHODOLOGY

A. Working Principle

The proposed system implements consortium blockchain concept to add nodes which are reputed institutions.

In consortium blockchain the nodes have to be verified first to build trust. Activities like mining, validation are carried out by these nodes only. The chain may or may not be public to view. Each node maintains its own off-chain storage to store records. But the updating in these off-chain databases relies on the blockchain ledger maintained by the peer-to-peer network. The communication among these nodes takes place with the help of RabbitMQ message broker service which enables asynchronous message transfer.

B. System Model

In the prototype of our system, we created nodes using Flask, a python web framework. Each node has access over a MySQL database. Only respective nodes have access over the MySQL databases. Each node also maintains a RabbitMQ server which takes part in the mining process. The whole peer-to-peer network maintains a central service which carries out some mining related activities. The central service and the nodes interact with a separate RabbitMQ server which is at the core of mining.

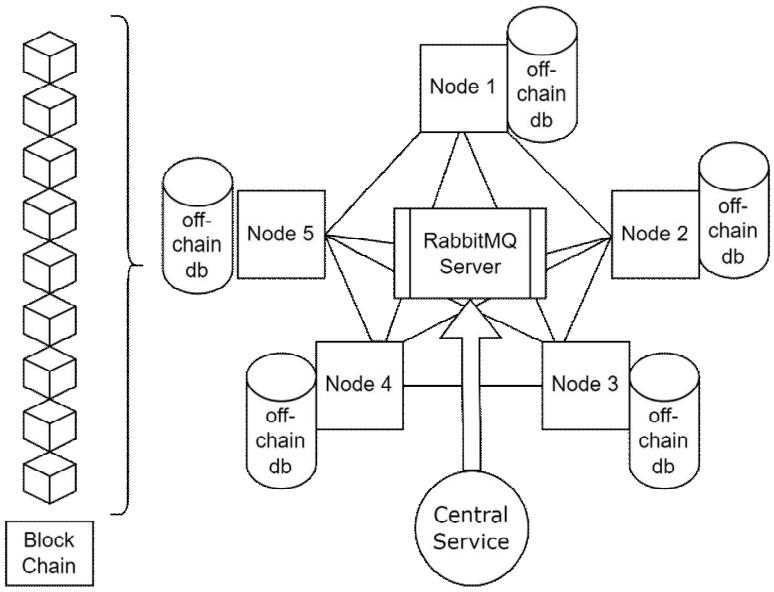


Fig. 1 System Architecture showing all the components

C. The Mining Process

Every node contains a temporary database as well as the main database which stores the actual records. A thread keeps running which constantly checks for existence of a record in the temporary database, say temprec. As soon as a record is found the node requests the name of the RabbitMQ queue to transfer this record in an encrypted form. The Central Service creates a fixed size queue on the RabbitMQ server which is not particularly associated with any node with unique name and broadcasts it to every node in the peer-to-peer network. Therefore, any other node may also transfer records to the same queue.

Once the queue reaches its limit no more messages are published to avoid any loss. The Central Service uses *Fisher–Yates* shuffle algorithm to decide a miner. Here, traditional consensus mechanisms are not being used as the nodes are assumed to be trustworthy. The miner node then starts consuming the supposed queue. Every node is given opportunity to become a miner. Therefore, a node may be able to mine transactions of other nodes and its own as well. The message in queue contains four components: *cur_hash* is the sha256 hash of student id and his results which are currently stored in the database and the blockchain as well; *future_hash* is the hash that would be stored on the blockchain if *cur_hash* matches with the hash in chain stored for *student_id* for the event *exam_type*. If the given condition is satisfied a positive response is sent back as reply to the sender queue. The positive response messages are temporarily stored. Otherwise, a negative response is sent back. The queue, in this way, behaves as a pool of messages, which is a basic feature of RabbitMQ. On processing predefined number of positive responses, a block is mined using them.

In order to consume these responses, the node also maintains a RabbitMQ server. On receiving a response for a message which is a record from the sender's perspective is, the record with positive response is updated and committed to the actual database. Therefore, a node can take on two roles at the same time. Here multiple blocking methods are involved so major modules run in separate threads.

Each node has response queue defined on its own server which whose consumption process runs in a separate thread. The message publication also requires a separate thread as well as a separate channel to avoid any overhead while interacting with external RabbitMQ queues.

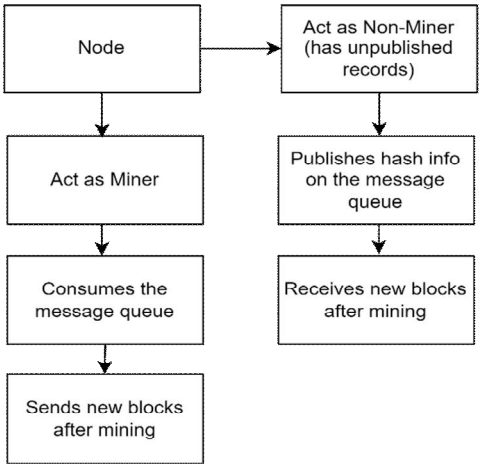


Fig. 2 The roles of a node in the p2p network

After the miner node has consumed all the messages the queue is deleted. The miner node broadcasts the new blocks to the network in order to update the chain. The block has the identity of miner included with its data which can endanger a node which maliciously broadcast false nodes.

D. Verifying a record

Verifying a record requires three things: the unique user id of the student and the *exam_type* parameter and the actual marks which may be obtained through some digital copy. By providing these as input to the network interface the hashes will calculated and compared. If a transaction exists for these parameters then it will return a positive response code. And in case the marks are not identical to the records in the off-chain storage (assuming the off-chain storage is perfectly consistent) or the ones that were used during the mining process, the response obtained is negative.

III. LITERATURE SURVEY

EduRSS [1] proposes a blockchain-based scheme for storing and sharing educational records. Blockchain technology is used to ensure data security and reliability, while smart contracts regulate the process of storage and sharing. The original records are stored on off-chain storage servers in encrypted form, and their hash information is stored on the blockchain. The records are periodically anchored to the blockchain to ensure data security. Cryptography techniques are used for records encryption and digital signature. The scheme consists of educational institutions, consortium blockchain, storage server, and framework service. The educational institutions are responsible for data storage and sharing, the consortium blockchain stores summary information of encrypted records, and the storage server encrypts and stores original records and files. The framework service provides functional modules to users through RESTful APIs. In order for an education institution to join the blockchain network proposed by EduRSS, it has to set up a blockchain node and register with the Certificate Authority (CA) to obtain its public and private keys. The official information of institutions is also stored in the CA. The CA serves as a key initializer and a mediator for the interaction between the external node and the blockchain member nodes, maintaining the security of the network through identity authentication and sanctions on malicious nodes. The role of the CA does not conflict with the blockchain, but rather complements it.

[2] proposed high-level architecture for a blockchain-based paper review system that uses IPFS file storage and access mechanisms. The IPFS system stores all papers, reviews, and review metrics files, and users can access them using respective fingerprints from the blockchain system. The IPFS file system is a distributed file storage system that uses a content-related hash code to allow users to access files from multiple sources. The proposed system has three types of files stored using IPFS: research papers for review and published full papers, review metrics, and reviews written by chosen reviewers. The advantage of using IPFS to store large file types is to reduce the size of the blockchain and to allow it to function faster and more efficiently.

AcadCoins can be rewarded to the reviewer as payment for paper revision. In the future, a detailed definition of open metrics will be proposed, and a plagiarism detection system will be included as one of the processes of paper review. The article also proposes adding an author's rating to the review document to increase the reviewers' motivation for writing meaningful reviews and increase the overall review rating accuracy.

[3] discusses the difficulty of analyzing blockchain protocols due to their large scale distributed networks, and proposes a queueing network-based method for analyzing consistency properties of consortium blockchain protocols. The proposed method is able to evaluate the performance of the main stages in blockchain consensus, and is applied to the Hyperledger Fabric system to recover key properties of the blockchain network. The article focuses on the three key stages of consortium blockchain protocols: execution, ordering, and validation, and analyzes the security properties of the ordering mechanism and the impact of delaying endorsement messages. The proposed method provides a more rigorous analysis of consortium blockchain schemes and allows designers of future blockchains to improve their protocols. The article also includes a diagram of the architecture of a consortium blockchain network and describes the three major components: client applications, peers, and ordering service.

[4] proposes a Decentralized Loan Management Web Application (DApp) built on the Ethereum blockchain. The aim of this DApp is to prevent fraudulent attacks on loan sanctions by decentralizing the loan process. The system implements security features such as user authentication, bank official authentication, and multiple levels of verification of details using Public Key Infrastructure (PKI). Smart contracts help in exchanging valuables, shares, properties, and money without any conflicts, and they eliminate intermediaries such as broker fees. The concept behind the smart contract can be easily described with the technology description of a vending machine. The Smart Contracts in DApps enforce obligations in addition to defining rules and charging penalties for the created agreement.

The proposed loan management system based on blockchain aims to securely share details about transactions by organizing the network, which helps prevent fraud in the system. The system maintains the privacy of valuable customers by eliminating attackers or frauds who inject vulnerable data. With this proposed system, banks in India can be completely digitalized without hesitation from hackers and attackers. The integration of blockchain in the loan management system incorporates easier, faster, and cheaper solutions, which can be adapted by existing banking systems for experiencing high-level security and privacy.

IV. RESULTS AND ANALYSIS

The performance of the network is enhanced by using multithreaded approach. The mining process can be improved by using multiple queues and multiple miners consuming them. However, this may not be required as the frequency of the need of updating educational records is not regular. RabbitMQ is a trusted message broker as it also supports cloud operations. The data transferred for the mining is cryptographically secured so the data leakages in this particular phase are not harmful. However, the privileges allowed to the Central helper service should be After the miner node has consumed all the messages the queue is deleted. The miner node broadcasts the new blocks to the network in order to update the chain. The block has the identity of miner included with its data which can endanger a node which maliciously broadcast false nodes.

V. CONCLUSIONS

The Hence, we have developed a blockchain network to store and verify the educational records by using a message broker service. As the ledger is shared by all the nodes, verification process becomes independent of the issuing node however in case an incorrect record is mined due to human error, new record from the initial exam_type need to be mined. One of the key benefits of using RabbitMQ in such a decentralized network is that it can ensure that messages are delivered reliably and in order. Messages may be lost or delayed due to network issues. RabbitMQ can help ensure that messages are delivered to the intended recipients, even if some nodes are offline or experiencing network issues.

REFERENCES

[1] H. Li and D. Han, "EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme," in IEEE Access, vol. 7, pp. 179273-179289, 2019, doi: 10.1109/ACCESS.2019.2956157.

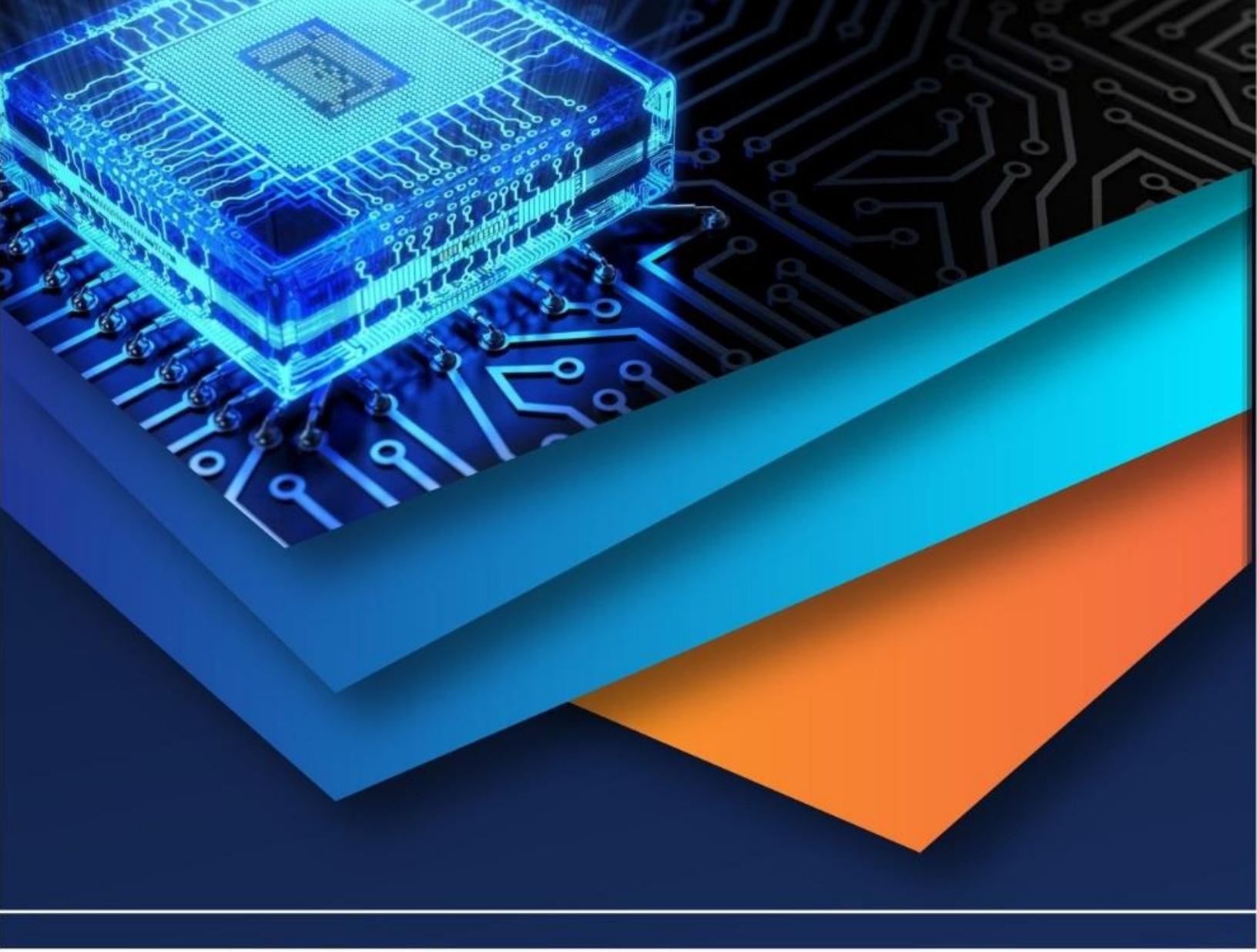
[2] Zhou, Ian & Makhdoom, Imran & Abolhasan, Mehran & Lipman, Justin & Shariati, Negin. (2019). A Blockchain-based File-sharing System for Academic Paper Review. 10.1109/ICSPCS47537.2019.9008695. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[3] T. Meng, Y. Zhao, K. Wolter and C. -Z. Xu, "On Consortium Blockchain Consistency: A Queueing Network Model Approach," in IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 6, pp. 1369-1382, 1 June 2021, doi: 10.1109/TPDS.2021.3049915.

[4] K.S.Arikumar, & Kumar, Deepak & GowthamC, & SahayaBeniPrathiba,. (2021). Decentralized Loan Management Application Using Smart Contracts on Block Chain. 10.3233/APC210020.

[5] Alammary A, Alhazmi S, Almasri M, Gillani S. Blockchain-Based Applications in Education: A Systematic Review. Applied Sciences. 2019; 9(12):2400. https://doi.org/10.3390/app9122400

[6] Chelladurai, U., Pandian, S. A novel blockchain based electronic health record automation system for healthcare. J Ambient Intell Human Comput 13, 693–703 (2022). https://doi.org/10.1007/s12652-021-03163-



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY