Integrity and Authenticity of Academic Documents Using Blockchain Approach

Mukul Rane[1,*], *Shubham* Singh[2,**], *Rohan* Singh[3,***], and *Vidhate* Amarsinh[4,****]

[1]Ramrao Adik Institute of Technology, Nerul
[2]Ramrao Adik Institute of Technology, Nerul
[3]Ramrao Adik Institute of Technology, Nerul
[4]Ramrao Adik Institute of Technology, Nerul

Abstract. Blockchain has a strong capacity to monitor and retain educational records. The paperless future has yet to become a reality, even with the ability to digitally generate documents. Physical copy of records are still regularly printed which makes them susceptible to document fraud. Thus, the issue of fake certificates and academic records has risen drastically. In this paper, we have made a reliable verification method to avoid academic frauds. The idea presented here is developed over Hyperledger. The University or The Educational Institute is responsible for issuing the certificates, mark-sheets, transcripts, etc. and mining it over the blockchain. The student is provided with the hash number which is the reference number. This number serves the reference of the data. The Organization or the Industry Personal using the hash number checks for the integrity of the submitted document. The present study discusses about importance of block chain and it's applicability especially for the applications like verification of Academic Records.

Keywords- Blockchain, Hyperledger, Academic Record Verification, Secure Hash Algorithm (SHA-256)

1 Introduction

Each corporation has critical information that demands protection. The current centralized storage system is the one that requires preservation of the information residing on the single system. Alternately, unless the content changed in the system the revised file is obtained by anyone who has to be stopped from doing so. Blockchain technology lets enterprises save the contents in every network-connected device. With such an approach a file can never be easily changed to store information [11]. For instance, whenever a file is changed in a system, it can never be updated on all network services since each service has its own version preserved in a database defined as a decentralized and distributed ledger [1]. Because the data contained in blocks and then each block is ultimately connected to another forming a block chain, the network is known as a blockchain [2]. The primary use of this application would be to prohibit participants or associations of external parties from entering into a contract. Digital currencies like Ethereum, Bit-coin, etc. emerged with the support of blockchain technology [3]. This can be the potential method of making a contract that involves only creator and recipient, excluding third parties. A contract can occur as a result of transfer of money, certification etc.

A blockchain is simply a digital log ledger which stores theoretically all types of information, such as payments, agreements, and occurrences. The processing of data occurs along a peer-to-peer platform, and is stored in electronic chunks sequentially [4]. Blockchain is rendered open, stable, decentralized despite nearly limitless storage capacity by such simple functionality [2]. Blockchain employs the hashing principle. The "hash" is a block fingerprint which takes into consideration all concerned data and logs. In short, a hash cryptography function considers an source sequence and renders it a special n-digit sequence [5]. The members on a network maintain their separate ledgers as well as other documents using conventional approaches for documenting logs and monitoring assets. This conventional approach can be costly, partly because it requires mediators paying their support for commissions. Due to problems in implementing negotiations and the proliferation of reporting needed to maintain multiple ledgers it is obviously inefficient. It is also insecure because when a centralized infrastructure is breached due to mismanagement, cyber attack, or a mere error, this affects the entire corporate network. Blockchain has a list of key attributes to overcome or boost standard approach: agreement, provenance, referential integrity and permanence. Every relevant members make choices by agreement, all stakeholders should consent to a contract being legitimate throughout this phase. Such objective is accomplished by bringing acceptance architectures into effect-infrastructure imposes the criteria whereby contracts can take place, or perhaps the sharing of objects that take place. Origin ensures audiences are mindful of whether the object derive from and the possession has changed significantly. No

*e-mail: rane.mukul@gmail.com
**e-mail: singh.shubham.16ce1034@gmail.com
***e-mail: rohansingh8174@gmail.com
****e-mail: vidhate.amarsinh@gmail.com

individual will, with absoluteness, tamper with a contract once it has been reported to the log. When a settlement is in mistake, the inconsistency should be replaced with something like a new transaction, and both transactions will then be clear [1]. A single common ledger essentially offers one way to ascertain the possession of an object or the conclusion of a transfer.

The existing Student Management System requires constant assembly between schools and organisations. With centralized data storage methods, the current university system is not successful. Student Management System can be applied to avoid the abuse of student information which is the most relevant blockchain application. The ledger application or blockchain framework uses its attributes such as confidentiality, atomicity and collaborative way of preserving information to establish a strong pavement for Student Management System implementation [6].

Academic databases are used globally, from the recipient's perspective, a valuable trait for entities promising for grants, employment, and overall teaching and research traction. Our academic database management software are generally largely geographically decentralized, require additional and un-trivial techniques for accessing records, are inefficient in several situations, and generally do not meet academic outcomes. Hence there is a need for a technology which encounters the forgery of the Academic Records and maintain the integrity of documents.

2 Literature Review

In this paper we presume that student records are stored in blockchain network form. Consider a situation in which one student has entered another educational institution. Student Managent System allows the students to validate the international or new university certificates. The paper indicates that the student has a wallet containing the certificates or details about the finished courses [7].

Once the student is about to enter a university of higher education, the institution will join the network and will validate the student's certificates. The 2-2 multi authentication protocol is used for verification process. The paper addresses the existing information disparity between the colleges and employer companies, an inadequate student credit scheme. Blockchain technology can help ensure accountability, validity and applicability of knowledge [8].

Smooth collaboration between students, academic institutions and employer organizations is achieved, enhancing the use and accountability of educational and job organisations. The paper explains an implementation of blockchain technology which is a trust-free framework called Bitcoin. A Peer-to-Peer network framework is suggested for money exchange. There is no need to identify peers because, in their interest, they can still quit and join the network. Blocks that are a transaction record are formally accepted or confirmed by casting a vote with the peer's CPU. The consensus mechanism will implement any rules and incentives the are required [9].

Using technologies like OCR, cryptographic hashing, digital signatures and 2D barcodes the integrity of the hardcopy documents was verified. Although forgery detection and integrity assurance was achieved the techniques involved were expensive and paperless environment was fully not achieved[10].

In this paper, they have used private permissioned blockchain instead of public blockchain as private permissioned blockchain gives higher performance, cost effectiveness as well as privacy. The main advantage of this paper is that in this the system is open and can be extended to any record type according to the specifics requirements of individual institutes. The drawback of the system is that it is only directed towards academic institutes. Other organizations and industries are not included[11].

3 Problem Statement

Presently the Student Management System is not secure against the document forgery. Fake documents as well as certificates are still being used at various levels. Hence we need a system which not only ensures the integrity of the documents but also maintains the authenticity. This proposed methodology proposes a system which is to be developed over a consortium blockchain. The issuing authority uploads the data by mining a block in the blockchain. Transparency is maintained as the end-user i.e. the industries or corporate officials can check for the integrity of document mentioned.

4 Proposed Methodology

Firstly the College or University authority issues the certificate, marksheet, transcript or any other document for the student and uploads it over the blockchain. After uploading the document, a hash key will be generated corresponding to that document. The student whenever submits

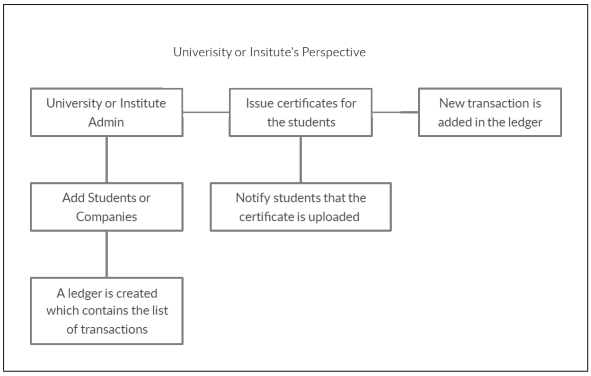

Figure 1. Block Diagram -Part 1

the document can also provide the hash number or the reference number to the Company which completely eliminates the need of the physical presence of the document and it also maintains the integrity of the document.

The Company or the Industry Personal can verify the document by just comparing the hash number or the reference number which is provided by the issuing authority. The approach comprises of dual main processes which are

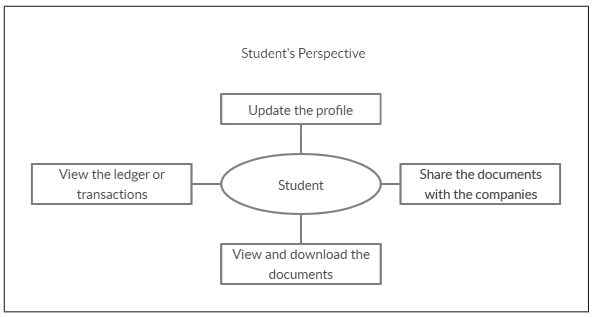

Figure 2. Block Diagram -Part 2

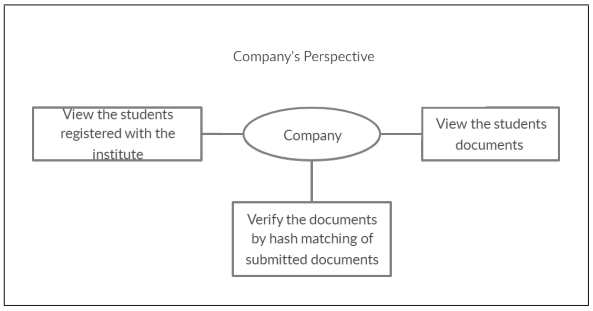

Figure 3. Block Diagram -Part 3

process generation and process validation.

• Generation Process: In this process, if the student wants to upload his documents, he will contact the co-ordinator. The co-ordinator will then log into the registration system to initiate the transaction. Then the co-ordinator will get all the relevant information of the student and the documents that student wants to upload. The documentation like the student's name, the title of the certification, the grade, the time-stamp, etc. is the block's content, using integer 9 computation. The block is ultimately tested using cryptographic strategies by previously selected nodes from the channel. The block is marked and attached to the blockchain system, such that all the users can reach the very similar chain, so that every node individually creates its very own example and indeed the hash is computed using the above process.

• Validation Process: Only after the records were produced, processed and released, the receiver can avail oneself of the same records in different situations, i.e. seeking employment, enrolling for assets etc. While these records are presented, they should be confirmed to evaluate if they have retained their credibility. Clients can post either a digital version, or a printed version paper. When displaying a paperback report, the report should first be scanned for a electronic copy to be accessed. The hash produced during the first step is used to commence the verification process [12]. The hash is determined contrasted to the one used in the actual file(retrieved through blockchain). If the analogy fails, this implies that the text has been changed. Although the checksum of every text label is computed, the hash value is also considered which helps in determining the forged text [5].

Algorithm required in this system:

SHA256: Tasks within the cryptographic computation of SHA256 are conducted onto terms which are 32-bit long using 8 terms of functioning variables such as P, Q, R, S, T, U, V and W which are of 32-bit. The term size of SHA256 measurement is, therefore, 32 bits. The characteristics for such functioning elements are determined for every computation and the SHA256 Cryptographic hash function has indeed been completed this process continues up to 64 cycles. Rationally, it should be remembered under all circumstances that certain changes in the SHA256 hashing computation are done with modulo 232.From here on out, the recipient will transform most of the increments described in the above material as increments conducted modulo 232 SHA256 also provide a 256-piece IV that is set for the main message square. A transitive digest message accumulated towards the completion of the preliminary 64 cycles filling in there as the square for the text. Post 64 iterations of the text pressure power and measurement extension, a midway message condensation of 256 bits is distributed along such lines. Once you have hashed the entire text squares, you get an advantage on 256 bits that is the last text analysis of the knowledge file. Therefore, the SHA256 cryptographic computation is virtually similar to a square figure with something like a 256-piece text square scale as well as a 512-piece key (data obstruction) penetrated into 64-bit 32-bit cycles keys using the text scheduler in each of the 64 cycles of such an example [13].

5 Implementation and Results

The current Student Management System is not efficient as providing fake documents is a big issue which is being faced. The verification of this fake documents if done is a hectic process as no dedicated system is present and it has to be done manually.

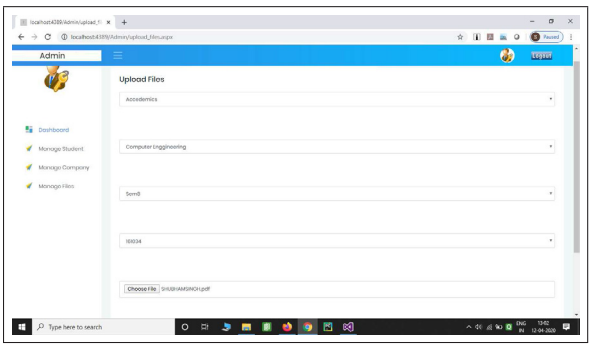

Figure 4. Admin Uploads Files of the students.

Hence if done manually, it requires at the least one day however if done for many students it can even last for

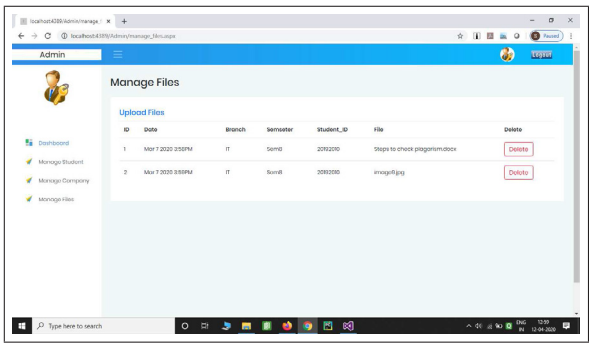

Figure 5. Admin can manage the uploaded files by deleting it.

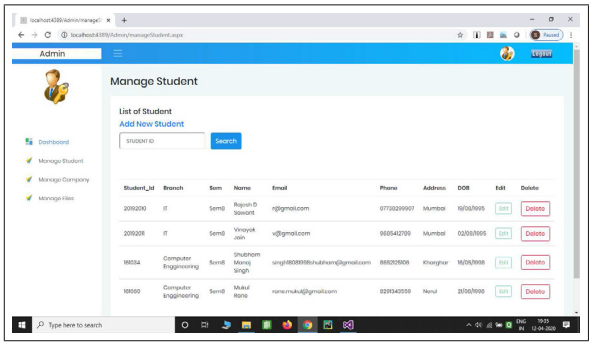

Figure 6. Admin can add students as well as Companies

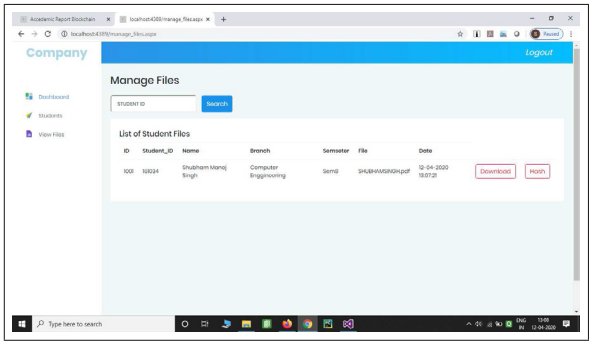

Figure 7. Companies can view the files which are uploaded over the site.

weeks which is really a time consuming process. Previously, a case had been observed where a slot of students who were about to join a company were required to verify the documents submitted during the background check. The authority concerned for verifying the documents had to contact the institute and put the joining of the slot on hold until the documents were verified. This process took few days for completion and the students had to wait until then. Including the faculty from institute and the verifying authority everyone were fully involved in this task which is tedious and soporific. By adapting to the proposed system, the time taken to verify the documents would be reduced to few minutes. The model has been tested on a group of students and it was reviewed to be reliable and fast.

After surveying a group of 100 students who had no such

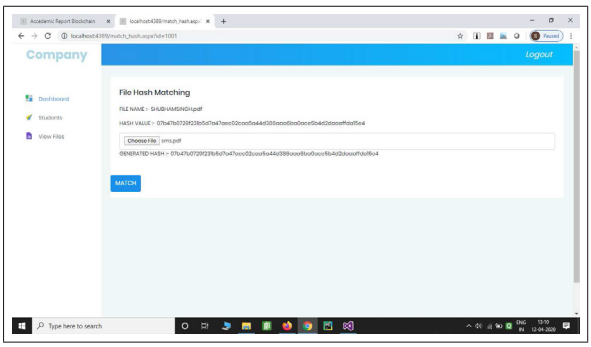

Figure 8. Company can compare hash value of files for ensuring the integrity

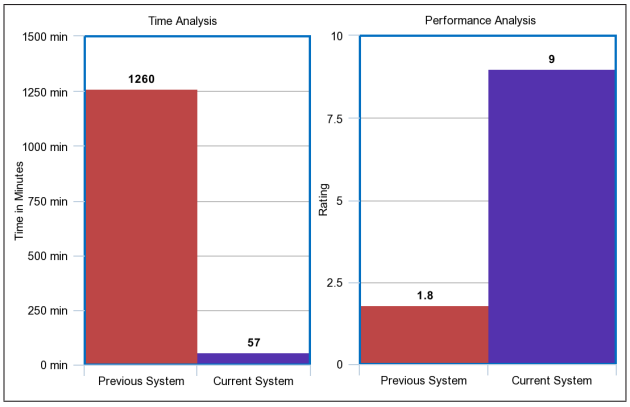

Figure 9. Analysis Graph

reliable system for verification of their documents, they had to provide the hard-copy of the original documents and move from one desk to another for completing this process which was really a hectic and frustrating process. Although if the process is done online there is no security as the documents could be edited and there is no tamper proof mechanism into use. In the same case the companies has to handle the huge crowd and perform the document verification on time but actually verifying the documents by making any call or over any other mode of communication is time consuming as sometimes the faculty is too busy to handle this request. The blockchain application has added an extra level of security as editing the documents is impossible here, thereby assuring the documents to be tamper proof. To verify our claim, we have surveyed 100 students to provide their feedback on both the systems. Average rating given to the previous system was 1.8 while our proposed system got 9. They found our system very user-friendly, time efficient and responsive.

6 Conclusion

This idea or program pays lip service to the transition problem and introduces a framework for checking college records among colleges and universities. Utilizing Hyperledger like a proprietary approved blockchain, offers higher output, benefit-effectiveness, including confidentiality contrasted with approaches for shared blockchain.

The program is indeed flexible and may be applied towards any form of records as per the specifications of every other organization. Although our system gives a convenient-to-use and reliable approach, ubiquity by various institutions is necessary to attain the mass momentum needed. Even if this is primarily aimed at academia, it would be easily adapted by including institutions seeking to verify potential job seekers' qualifications. The program can also be modified to exploit and modify current solutions, like serving as something of a network broker (i.e. cross border and global).

It is proposed to use blockchain in the student management system to preserve student information using blocks and also to accept student accomplishments and university qualifications. This idea can be implemented in upcoming time by suggesting a method to create a fully functional system that includes attendance, student marks, receipts for student payments towards the university.

7 Future Work

The further enhancement of the proposed methods can be focused on the following ideas for ensuring better performance and widespread applicability of the application. Firstly, the proposed system is implemented only for single institute. Hence, this system can be scaled to other institutes. More participants would be able to use our system. Secondly, notifications can be given to the student whose document has been uploaded over the Blockchain. This notification can be as an email or text message over mobile phone.

References

[1] O Nathan and P Alex Sandy. *"Decentralizing privacy using blockchain to protect personal data"*. SPW 2015 IEEE (2015).

[2] P.S.G. Aruna Sri and D.I. Bhaskari. *"A study on blockchain technology"* IJET(2018).

[3] J. Sidhu *"Syscoin: A peer-to-peer electronic cash system with blockchain-based services for e-business"*. IEEE(2017).

[4] K. Jay and A. Akutsu. *"The blockchain-based digital content distribution system"*. ICBDC IEEE(2015).

[5] Bart Preneel. *"Cryptographic Hash Functions: Theory and Practice"*. Springer-Verlag Berlin Heidelberg 2010).

[6] Sushmita Ruj and Kwok-yan Lam. *"A Blockchain framework for insurance processes"*. BSC, IEEE (2018).

[7] Aida Kamiali, Kristjan Koi and Marjan Heriko. *"Eductx: a blockchain-based higher education credit platform"*. IEEE ACCESS (2018).

[8] Gill green, Qin Liu and Hongming Zhu *"Education-industry cooperative system based on blockchain"*. HOTICN 2018, IEEE (2018).

[9] Satoshi Nakamoto. *"Bitcoin: a peer-to-peer electronic cash system"*.

[10] A Permissioned Blockchain-Based System for Verification of Academic Records *"https://ieeexplore.ieee.org/document/8763831"*

[11] Proposing a Blockchain-based Solution to Verify the Integrity of Hardcopy Documents *"https://ieeexplore.ieee.org/document/8601200"*

[12] M. Nakasumi. *"Information sharing for supply chain management based on block chain technology"*. IEEE CBS 2017.

[13] Matsui M., Zuccherato R.J. *"Security Analysis of SHA-256 and Sisters"*. Springer, Berlin, Heidelberg, 2004.