

Automatic Digital Degree/ Documents Verification Using Ethereum Blockchain

¹ Roshani S. Bele, ² Jayant P. Mehare

¹M.Tech. Student, Department of Computer Science and Engineering, G H Raisoni University, Amravati, India

²Assistant Professor, Department of Computer Science and Engineering, G H Raisoni University, Amravati, India

Email - ¹rinkubele1995@gmail.com, ²jayant.mehare@raisoni.net

Abstract: *In the present education system, about 37 million students were enrolled for graduation every year in India. After completing their studies, some of them prefer to go abroad for higher education while others are ready to take up employment in the workplace. During this process, the falsification of documents becomes a major problem. The document verification is a complex area that involving various challenging and lengthy processes for the authentication. The blockchain technology provides an opportunity to create new academic models and solve forgery problems efficiently. Therefore, this technology has potential to lead many research opportunities and Academic Innovations. Here, we have to be presented a system design process work will to be used in the decentralized an application for a certificate verification system based on the blockchain technology. According to the statistics of the Ministry of Education (MOE), previous degree certificates are additionally verified manually by college authorities during the admission process and by third parties during the interview process. This process requires a lot of time and the manpower. During this process, to solve the problem of the certificate forgery, using the digital certificate system based on the blockchain technology. In this research, the authors have identified the security issues required for the document verification in the blockchain. This research also identifies the forgery issues in the current Blockchain based the educational certificate verification solutions.*

Keywords: *Blockchain, Cryptography, Digital Certificate, Hash Code, Transaction.*

1. INTRODUCTION:

Nowadays, daily life of university students is evolving more and more into the digitalized form. This is also true for the digital degree certificates produced by the universities, university authorities and various job applications, which contain all the degree-related information. Universities issue the certificates to students after they have graduated. A degree certificate is usually an important part of the student, but a degree certificate in the form of a paper-based document, an electronic document cannot effectively replace a physical certificate. During this process, due to the existence of advanced and cheap scanning and printing technologies, the forgery of certificates has increased during their life, students come in contact with a large number of employment agencies or jobs. Each of them stores this personal data in their respective information technology systems (IT), resulting in a fragmented system and databases that are not interconnected. Certificates are important for students when applying for jobs, whether in the public or private sector. They are usually produced in a paper form and are difficult to keep. Issued certificates need to be manually verified, which are very time-consuming and costly. Therefore, the efficiency of the system can be increased by the digital certificate verification based on the blockchain technology.

In this paper, we propose an innovative model of a certificate verification system based on the privacy preservation. In this model, users have a control over their data and are recognized as the owners of their own data. They can apply various security policies such as releasing data with the certificate verification, and documents such as results, academic Credentials, etc. can be submitted to various authorities that verify them in a detail. The verification time is considerably high, so this time-consuming a task should be minimized.

A blockchain system stores student records permanently so that these documents, such as degrees and course certificates, can be securely verified whether a user has access to an institutional system of the record. A system is using the blockchain technology is continuously growing a chain of blocks, each of which contains a cryptographic hash of the previous block, a timestamp, and the data will to be transferred. Due to the existence of the cryptographic hash, the data have stored in a blockchain are inherently resistant to the modification; if a block of data is modified, all blocks should subsequently be regenerated with new hash values. This property of immutability is fundamental to blockchain applications.

2. MOTIVATION, AIM, OBJECTIVE:

From last few years online academic Process increases rapidly, so there is need to organize and manage all data online and to save that data in single place from which we can easily retrieve that data during this process occurring the counterfeit university mark card has been a recognized problem in the field of educational society. To overcome this problem and secure the certificate using decentralize application blockchain technology.

Aim

“We aim develop a decentralized application for a certificate system based on public blockchain. This technology was selected because it is incorruptible, encrypted, and traceable and permits data synchronization. By integrating the features of blockchain, the system improves the efficiency operations at each stage.”

Objective

- To implement block chain mechanism to minimize document verification time.
- To develop an application for a certificate verification by realizing concept of public blockchain.
- To integrating the features of blockchain, in the documents verification process for validation system which leads to reducing time complexity.
- To improves the efficiency and traditional approach in certificates verification.
- The prime objective of our system is to implement document sharing and validating it without increasing management costs also it prevents document forgery that provides accurate and reliable information on digital certificates.

3. RELATED WORK:

In a Blockchain technology each block is linked to another block in a chronological time-stamped a manner simply as data structure. Blockchain is a large and openly accessible online ledger where each node stores and verified the same data. The each every record is validated across the distributed the network before being stored in a block. All information has once stored in the ledger is verifiable and the audit able but not editable. Each every block is identified by its signature. In the blockchain of the first block is also called as the genesis block. The use has of the proposed the blockchain-based the system reduces the probability of the certificate forgery.

The process of certificate application and the automatic certificate issuance is open and transparent in the system. Therefore, companies or organizations can retrieve information about any certificate from the system. Data security is one of the most important features of blockchain technology. Blockchain is a decentralized data storage mechanism where all transaction data (stored in nodes) is added to different blocks. Blockchain is basically divided into two types: public blockchain and private blockchain. A public blockchain is decentralized and has no single entity controlling the network and the data is publicly available, while a private blockchain operates based on access controls that restrict who can participate in the network. In 2013, blockchain technology evolved with the advent of Ethereum Smart Contracts, which became Blockchain 2.0.

Decentralized Ledger: Blockchain no longer relies on a single central node such as a master node, each node can record, store and update the ledger, and together they form the blockchain. Decentralized Ledger technology describes digital databases where each member can contribute to the data stored there, not centrally in a cloud, but locally on each computer in the network, which functions as a decentralized peer-to-peer network. One of the features is the decentralized consensus mechanisms implemented by algorithms on the participating computers, this so-called mining verifies the data in the decentralized network and makes DLT transparent, secure and decentralized and thus the backbone for future transactions and verification processes. With the blockchain, a new digital block is written for each new data record with a distinctive signature that contains the hash value of the previous block

Ethereum: Ethereum is an open and decentralized platform has that featured Turing completeness. It also supports various derivative applications. Ethereum has been used to create most decentralized autonomous organizations as well as smart contracts. Ethereum can be considered as a global computing system as compared to Bitcoin blockchains which are considered as a global payment network. It is also similar to other open source platforms, such as Google's Android. Ethereum acts as the cryptocurrency that provides Ether tokens for users to create and deploy decentralized applications. It provides an infrastructure that allows developers to create applications. The infrastructure is developed and maintained by both Ethereum and these developers.

4. PROPOSED METHODOLOGY:

4.1 ANALYSIS:

This system is designed for verification of degree certificate and other documents. This system contains three functionalities.

USER1: User 1 is Document Creator /University, This user generates and issues any certificate for students. First the student's eligibility for the certificate is checked, then the certificate is generated and the hash of the certificate is calculated and uploaded to the blockchain. User 1 generates the certificate for the student and displays it.

USER 2: User 2 is student/ Document Owner, This user qualify some exam, port to get certificate from user 1. User 2 take two decision, user 2 share certificate with other users with their user ID and view the certificate and upload the certificate of user 1.

USER 3: User 3 is an authenticated third party/company. This user gets latest document copy from user 2 and need to verify it from user 1. user 3 request certificate from user 1 and user 2 and share certificate.



Fig 4.1. Use Case Diagram

4.2 SYSTEM DESING & PROCESS:

In this phase, the architecture is determined. In this step, the system is explained as shown in the figure below. The achievements of the students which are in the form of degree certificates, mark sheets, merit certificates etc. become an important weight for recruitment or higher studies. The awards and degree certificates of the educational institution may contain only the name of the institution and the dates of the student. In this scenario, there is lack of effective anti-fake mechanism, hence fake degree certificates are often found. To solve the problem of fake certificates, blockchain technology would store the certificate in digital form. The digital certificate verification system is developed as a decentralized application for a certificate system based on the public blockchain, showing that the issuer, i.e., the university (issuer), creates the certificate for the graduates. Generate the hash value for the certificate using the MD5 hash code. The fixed length hash value are stored in the block as a transaction. In the blockchain the transaction is validated by the members. Once it is accepted as a valid transaction, the block is added to the existing blockchain. The acceptance and rejection is done by a consensus algorithm. The consensus algorithm can be selected depending on the number of nodes and transactions. The system generates the associated MD5 hash code and hash code which is inserted into the hardcopy certificate. The system offers the possibility to authenticate the hardcopy certificate via the website. Due to the immutability of the distributed ledger, the system not only provides certificate verification but also stores the certificate forever in digital form.



Fig 4.2: System Design

4.3 IMPLEMENTATION & RESULT:

Nowadays, record keeping is a problem in educational organizations. During the interview process to show all records takes a lot of time, so it is better to sue all records stored in blockchain their hash value which can be easily available anytime and anywhere. Therefore, we provide a service to calculate the hash value of various files and store the hash value of certificates in the blockchain by using cryptographic solutions. The platform is designed to store the hash of certificates in the block. Once the certificate hash is stored in the block, it cannot be corrected or changed by anyone. Storing the information in the block also removes doubts about the employee's knowledge.

In this system, there are three types of users: user1 (university), user2 (student) and user3 (company). First, the student fulfills certain requirements, the authorities issue a certificate/result or other documents through the system. Then the student applies for the certificate, the issuing authority verifies the credibility of the student and issues the certificate and its block in the public blockchain. Secondly, the issuing authority needs to log in to the website, after verifying the correctness of the student details, they can upload all the documents (certificates/results) and calculate their hash values. The next step is uploading this hash value to the block of the public blockchain by the authority. Once the hash value of the documents is stored in the block, it cannot be changed by anyone. In the fourth step, any company that makes a request to verify documents can easily validate them. They need to upload the same documents to the website and generate their hash value. Once this hash value is generated, it must match the previous hash value uploaded by the authority to prove the validity of the documents. If the data of a document is changed by a student, the hash value generated by the companies will be different from the original hash value, which can lead to the detection of document forgery.

On the registration page, the user clicks on "Register now", enters his basic data and receives a confirmation e-mail (Fig. 4.3.1).

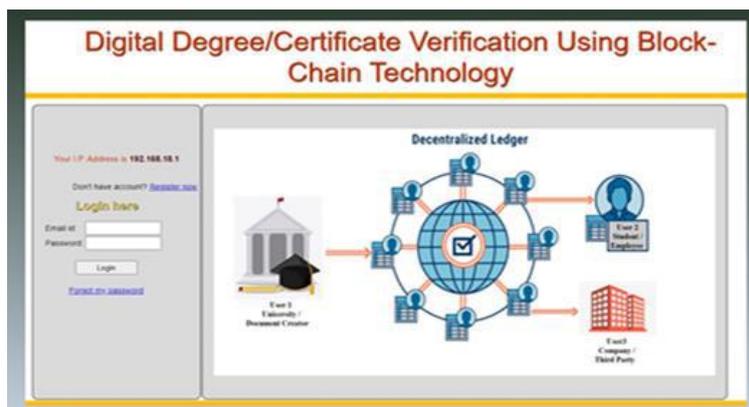


Fig. 4.3.1 Front page of the blockchain certificate verification system

The university is going to generate the degree here, now we're going to upload it to a file, now we're going to calculate a hash code that's going to be generated now as soon as you upload it. A document that is uploaded to the local server generates its hash code file in the leader of the at the same time blockchain.

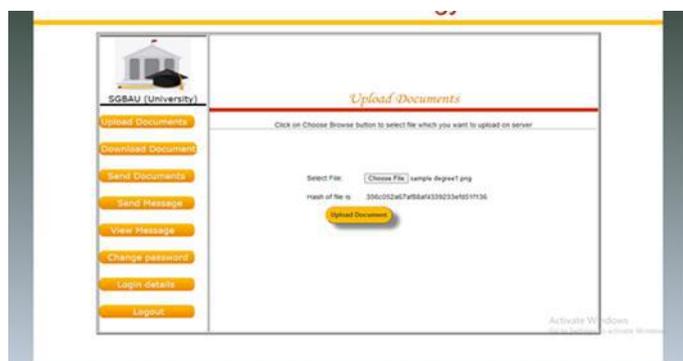


Fig 4.3.2: Upload documents

From here we can download the document and delete the full information and the file is hash code (Fig.4.3.3 and 4.3.4).



Fig4.3.3: Download Documents

After some change is done in sample degree so current file hash is changes.



Fig 4.3.4: Download Documents

When a company acquires a unique ID from a job applicant, it logs into the system to verify the authenticity of the associated certificate. The message "valid certificate" is displayed if the information from applicants matches the information in the blockchain system (Fig.4.3.5).

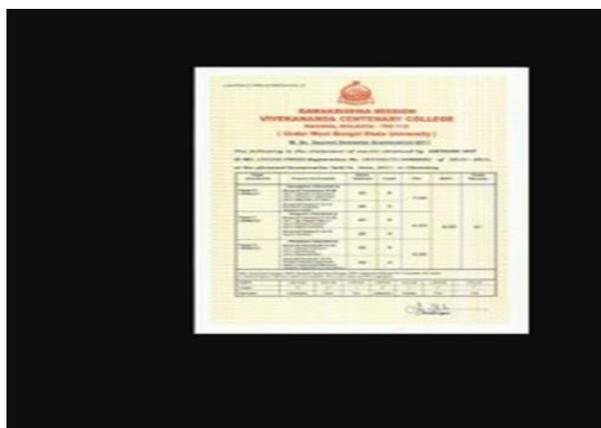


Fig4.3.5: Blockchain Successful Certificate Verification

5. CONCLUSION:

Various technologies have been discussed Blockchain systems use cryptography technologies, P2P networks, and consensus models to provide infrastructures for decentralized applications. A blockchain-based the graduation a certificate verification model was proposed to improve the verification mechanism. This will reduce the occurrence of the certificate forgery and improve the security, a validity and confidentiality of graduation certificates. The proposed model offers many benefits to issuing authorities as well as to recipients and consumers. In this research, we have shown how blockchain technology can be used for document verification and security. Our research shows that blockchain technology is capable of providing up to 85% security for educational documents. Therefore, Securecert, which was developed based on blockchain technology, added the additional security for students' assets by securing each certificate in the blocks. An improvement in the verification process has been proposed as a decentralized application blockchain model for verification of degree certificates. Blockchain technology can be used to avoid the risk of forgery of education

certificates, and there are many other applications as well. Traditionally, the easiest way to forge the document is to simply take someone else's document and change the owner's name on it. In today's world, blockchain is one of the leading concepts around the world. It is the potential to revolutionize the field of education society.

Future Implementation: For future work, the proposed model "Document Verification System" using Ethereum-based Blockchain can be implemented in educational/non educational institutions and enterprises where document verification is required. It can be further extended to be based on various distributed blockchains and smart contracts.

REFERENCES:

1. Ze Wang, Jingqiang Lin, Quanwei Cai, Qiongxiao Wang, Daren Zha, Jiwu Jing, "Blockchain-based Certificate Transparency and Revocation Transparency", PP(99):1-1 • March 2020,IEEE.
2. Mohamed Laarabi, Abdelilah Maach, Abdelhakim Senhaji Hafid," Smart Contracts and Over-Enforcement: Analytical Consideration on Smart Contracts as Legal Contracts",IEEE/978-1-7281-4979-0/20/IRASET.2020
3. Alexander Grech, Anthony F. Camilleri, Andreia Inamorato dos Santos, "Blockchain in Education", JRC Science Hub, ISBN 978-92- 7973497-7, and DOI: 10.2760/60649, 2017
4. Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi and Yi-Hua Chen. (2018) Blockchain and Smart Contract for Digital Certificate. Available: DOI : 10.1109/ICASI.2018.8394455
5. Wei Cai, Zehua Wang, Jason B. Ernst, Zhen Hong, Chen Feng and Victor C.M Leung. (2018) Decentralized Applications: The Blockchain Empowered Software System. Available: <https://arxiv.org/pdf/1810.05365.pdf>
6. Nitin Kumavat, Swapnil Mengade, Dishant Desai and Jesal Varolia. (April 2019) Certificate Verification System Using Blockchain. International Journal for Research in Applied Science & Engineering Technology (IJRASET), (Volume 7 IssueIV). Available: <http://ijraset.com/fileserve.php?FID=20914>
7. OsmanGhazalianOmarS.Saleh.AGraduationCertificateVerificationModelviaUtilizationoftheBlockchainTechnology.Available:<http://journal.utem.edu.my/index.php/jtec/article/download/4707/3640>
8. Guang Chen, Bing Xu, Manli Lu and Nian-Shing Chen. (3 January 2018) Exploring Blockchain Technology and its Potential Applications for Education.Available: <https://slejournal.springeropen.com/articles/10.1186/s40561017-0050-x>
9. Ali Alammary Samah Alhazmi, Marwah Almasri and Saira Gillani. (13 June 2019) Blockchain-Based Applications in Education: A Systematic Review. Available: <https://doi.org/10.3390/app9122400>
10. Rakibul Hasan Sayed. (2019)Potential of Blockchain Technology to Solve Fake Diploma Problem.Available:<https://jyx.jyu.fi/bitstream/handle/123456789/64817/1/URN%3ANBN%3Afi%3Aaju-201906253406.pdf>
11. RujiaLiandYifanWu.BlockchainbasedAcademicCertificateAuthenticationSystemOverview.Available:[https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockchain-based-Academic-Certificate-Authentication-System verview.pdf](https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockchain-based-Academic-Certificate-Authentication-System%20verview.pdf)
12. Gowri Shankar, Draavid, Kamesh, and Dr.Jaison. (March2019) Blockchain based Certificate Issuing and Validation. InternationalResearchJournalofEngineeringandTechnology(IRJET)(Volume6Issue3).Available:<https://irjet.net/archives/V6/i3/IRJET-V6I3369.pdf>
13. Benyuan He, "AnEmpirical Study of Online Shopping Using Blockchain Technology", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.
14. NeethuGopal, Vani V Prakash, "Survey on Blockchain Based Digital Certificate System", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 11, e-ISSN: 2395-0056 Nov 2018.
15. Esmat Mirzamany, Mansoor Hani, 'Blockchain: An Enabler of Efficiency, Choice and Agility in Education', JISC, August 2018
16. David McArthur, "Will Blockchains Revolutionize Education", 21stMay 2018.
17. L Morhaim, "Blockchain and crypto currencies technologies and network structures: applications, implications and beyond", September 6, 2019 version-1 Hal archive .
18. Cristiane Dias Lepiane , Fernando Lauro Pereira , Giovani Pieri , Douglas Martins , Jean Everson Martina , Mauro Luiz Rabelo "Digital Degree Certificates for Higher Education in Brazil", September 23–26, 2019, ACM ISBN 978-1-4503-6887-2/19/09
19. Liviu Hirtan, Ciprian Dobre, Piotr Krawiec, Jordi Mongay Batalla "Blockchain-based approach for e-health data access management with privacy protection" IEEE 978-1-7281-1016-5/19/ ©2019 ./CAMAD.2019