INTERNATIONAL JOURNAL ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

IJIEMR Transactions, online available on 10th Apr 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04

10.48047/IJIEMR/V12/ISSUE 04/144

Title **DIGITAL CERTIFICATE SIGNATURE VALIDATION USING BLOCK CHAIN**

Volume 12, ISSUE 04, Pages: 1130-1138

Paper Authors

R. Sudha Kishore, Pendela Sai Ganesh, Shaik Firoz, Tarun Siva Sai Gummadi,

Veluri Venkata Naga Sai Rohith

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

DIGITAL CERTIFICATE SIGNATURE VALIDATION USING BLOCK CHAIN

R. Sudha Kishore[1], Associate Professor, Department of IT,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.

Pendela Sai Ganesh[2], **Shaik Firoz**[3], **Tarun Siva Sai Gummadi**[4], **Veluri Venkata Naga Sai Rohith**[5]
[2,3,4,5] UG Students, Department of IT,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.
[1] sudhakishore@vvit.net [2] ganeshpendela30@gmail.com,
[3] firozshaik5891@gmail.com, [4] tarunmsdian21@gmail.com,
[5]velurirohith@gmail.com,

Abstract

Every year, approximately 6.5 million graduate students earn a degree in India. Throughout his studies, a student generates a large number of certificates, which may include transcripts, affidavits, and credentials'. Students must present these certificates to gain admission to universities or companies. Manually enquiring these certificates and validating their genuiness becomes time-consuming. The lack of a proper anti-forge system results in a situation in which the certificate is discovered to be forged. In order to enhance the security and safety of data, it is essential to convert all information into digital form and adhere to the principles of confidentiality and reliability. The system under developed consists of three stages. During the initial phase, the college will register students store and their credentials on the Ethereum block chain. In the subsequent stage, students will have the ability to view their certificates and apply for employment by uploading them. Lastly, during the third phase, corporations will be able to request access from colleges in order to authenticate the credentials they desire. Using hash functions, companies can verify certificates sent by both students and universities. The advantage of such a system is that the student the certificate can be validated quickly. The suggested system not only addresses the shortcomings of our current system but also presents us with a realistic and tangible resolution.

Keywords: Hashing Function, Block Chain, Digitalized, Confidentiality, Reliability.

Introduction

Document forgery is a growing issue that requires immediate attention. Over the past few years, there has been a notable rise in instances of fraudulent replication of certificates. Counterfeit certificates and false information are affecting the industry, particularly the IT sector, which employs a large number of people. As the percentage of graduates grows each year, it becomes increasingly difficult to keep track of and confirm such a large number of records. As a result, an unpleasant scenario emerges, namely tampering and the generation of counterfeit or duplicate certificates. Many covert groups within our nation are engaging in this deception without anyone's knowledge. Differentiating between a bogus and an actual certificate will take a lot of time and effort. To address this shortcoming, a technology known as Blockchain enters our lives as a solution.

Blockchain technology provides several advantages in the validation of fake certificates. One of the main advantages is that blockchain provides a decentralized, tamper-proof, and transparent platform for storing and verifying certificates. This means that once a certificate is issued and stored on the blockchain; it cannot be altered or deleted, ensuring the integrity and authenticity of the certificate. Since the blockchain is a decentralized platform, it eliminates the need for intermediaries such as third-party verification agencies, which reduces the cost and time required to verify certificates.

The proposed system employs block chain technology in conjunction with cryptography techniques to determine whether a certificate is genuine or counterfeit, eliminating the need for human intervention and saving a significant amount of time and effort.

Literature Survey

The project is focused on developing a certificate validation system. For this, we have viewed some previous scholarly articles and the writings of different experts in this particular field. Our literature review engaged primarily on Blockchain Technology, Cryptography, and Hashing Algorithms.

[1] This paper "An Overview of Blockchain Technology" gives in-depth information about Blockchain. It outlined different terms related towards this technology, including the most essential concept known as a smart contract. The hash value or checksum of the data is kept in the preceding block of the Blockchain, which forms a chain of nodes. If information has been altered, its hash value will get altered and will no longer match the hash code stored in the preceding block, indicating data tampering.

[2] The paper's "Blockchain and Smart Contract for Digital Certificate "structure included three key players: institutions, students, and a service provider. However, the flaw in their approach was the use of a single hash as a key, which rendered the information publicly available once the hash was obtained.

[3] This article "Tamper Proof Birth Certificate" bears resemblance to the second one in terms of design, with the exception that they utilized the Advanced Encryption Standard algorithm and

tailored their system for Birth Certificates. However, a downside that was noted is that the initial document was not saved in any location.

[4] The paper "Certificate Verification using Blockchain and Generation of Transcript"used the concept of block chain but there is no concept of hashing for identifying whether the certificate is original or fake. In extra they also generated certificates.

[5] The Last paper named "A system for Academic certificates using block chain"; in this paper the companies send access request to students to send their certificates and no hashing algorithm is used in this paper.

Problem Identification

The main problem of fake certificates is that they can be used to deceive or defraud individuals, organizations, or institutions. Fake certificates can be used to gain access to job opportunities, educational programs, or other benefits that require legitimate credentials. This can result in unqualified individuals occupying positions they are not qualified for, which can lead to poor performance, safety risks, or other negative consequences. Additionally, the issuance of fake certificates can damage the reputation of legitimate institutions and devalue the qualifications of those who have earned legitimate credentials. Fake certificates pose a serious threat to the integrity of the educational and professional systems that rely on trustworthy certification processes. So, to overcome this proposed system uses block chain technology in addition with cryptographic algorithms. One of the main advantages is that blockchain provides a decentralized, tamper-proof, and transparent platform for storing and verifying certificates. This means that once a certificate is issued and stored on the blockchain; it cannot be altered or deleted, ensuring the integrity and authenticity of the certificate. Moreover, the use of blockchain technology in fake certificate validation allows for a more efficient and cost-effective verification process. Since the blockchain is a decentralized platform, it eliminates the need for intermediaries such as third-party verification agencies, which reduces the cost and time required to verify certificates.

Methodology

A. SHA-256

The SHA-256 algorithm is designed to hash digital data, which includes images. When hashing an image using SHA-256, the image is first converted into a binary format, which consists of a series of 1s and 0s. The binary data is then processed through a series of mathematical functions to produce a unique 256-bit hash value.

The specific steps involved in hashing an image using SHA-256 are as follows:

1. **Convert the image to binary format**: Each pixel in the image is

represented by a set of binary digits, usually 8 bits per pixel. The entire image is then converted into a long string of 1s and 0s.

2. **Pad the data**: The binary data may not be an exact multiple of 512 bits, which is the block size used by SHA-256. Therefore, the data is padded with additional 0s until it is an exact multiple of 512 bits.
3. **Process the data through the hash function**: The padded data is processed through a series of mathematical functions that transform the data in a non-reversible way. These functions include bitwise logical operations, modular arithmetic, and rotation operations.
4. **Produce the hash value**: After all the data has been processed, the final output is a 256-bit hash value. This value is unique to the original input data and can be used to verify the integrity of the image.

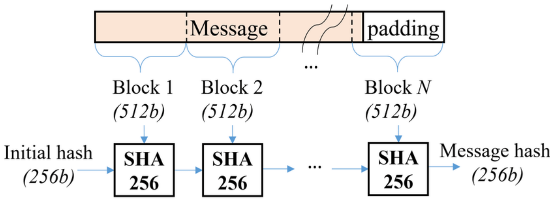


Fig.1. Generation of Hash Value.

B. Solidity Contracts

Solidity is an object-oriented programming language that has been specifically developed by the Ethereum Network team for the purpose of building and designing smart contracts on Blockchain platforms. Its primary function is to facilitate the creation of smart contracts that incorporate business logic and generate a series of transaction records within the blockchain system.

C. Ganache

Ganache is a personal blockchain for Ethereum development used for testing and development purposes. It provides a user-friendly interface and allows developers to test and debug their Ethereum smart contracts locally**.**

D. Truffle

Truffle is a popular development framework for building decentralized applications (dApps) on the Ethereum blockchain. It provides a suite of tools and libraries that make it easy to write, test, and deploy smart contracts and dApps.

F. Metamask

Metamask is a browser extension that allows users to interact with Ethereum blockchain applications by providing a secure wallet and identity management system.

Work flow of the project

Three people are involved in the proposed system.

1. **College**: The college team can login to the website and has the responsibility of entering student information into the block chain, such as name and student id. The

College serves as a certificate issuance authority. All of the information entered by the college is saved in a block chain. If a company requests that the college send the certificate of a specific student, the college may accept the request and send the certificate.

2. **Students:** College students can access the website and apply for job openings. After the company verifies the certificate, students will be able to view the decision. They are also able to view their certificate.
3. **Company:** The company can also login to the website and post job details such as the type of job, role of job, and salary for the specific role, and if any student needs to apply for the job, the student must enter the certificate, and the company decides whether to approve or reject based on the certificate provided by the university and comparing their hash values of both the certificates.

Implementation

The proposed system employs HTML, CSS, and Java Script for the front end. The backend is built with the JavaScript library node.js. Since the project deals with block chain software's like ganache and truffle are used. Ganache is a personal blockchain for Ethereum development used for testing and development purposes. Truffle provides a suite of tools and libraries that make it easy to write, test, and deploy smart contracts and dApps. Metamask is a browser extension that allows users to interact with Ethereum blockchain applications by providing a secure wallet and identity management system. Solidity is used to implement the Ethereum smart contract. Truffle is used to compile, deploy, and test the smart contract. Ganache is used to establish a local Ethereum blockchain to test smart contracts. Ganache provides ten accounts with fictitious ether that may be utilized for testing transactions.

The cornerstone of every blockchain initiative is the contract, which is essentially a software program that runs on an Ethereum node. These contracts are created using the Solidity language, which is derived from high-level programming languages like JavaScript and dynamically-typed languages that are primarily utilized for writing contracts. The code includes the contract file Migration.sol. The migration.sol file is the default solidity file that comes with the ethereum setup and consists code for how transactions should occur and how to keep track of transactions.

Another important file is the MerkleTree.js file which contains the code for the generation and comparison of the hash value. In this code, the createHash() function is utilized. This function belongs to the crypto module and enables the creation of a Hash object. This object can then be utilized to generate hash digests utilizing the algorithm that is specified. Here we used the SHA-256 algorithm to produce hash value.

The IPFS (Inter Planetary File System) is a crucial element of the system, enabling users to securely upload certificates. By using a distributed network where no single user is responsible for storing the document, the submitted certificates are protected and can be accessed through a hash. As the file is divided among multiple nodes in the IPFS system, it is impossible for anyone to access the document simultaneously.

Results

Login Page:

There are three different login pages one for student, other for company login and university login.

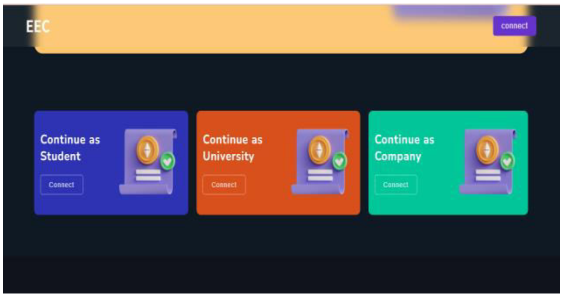
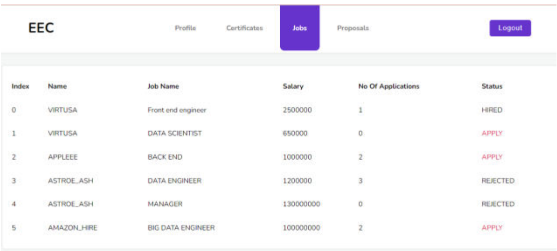


Fig.2. Login Page

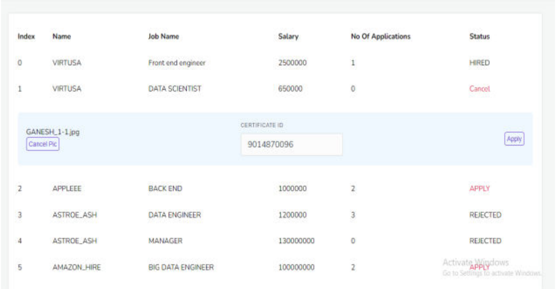
Student

The student after login using unique id and student name, has the options to view profile, request for certificates, apply for jobs by uploading certificates and view proposoals



Index	Name	Job Name	Salary	No Of Applications	Status
0	VIRTUSA	Front end engineer	2500000	1	HIRED
1	VIRTUSA	DATA SCIENTIST	650000	0	APPLY
2	APPLEEE	BACK END	1000000	2	APPLY
3	ASTROE_ASH	DATA ENGINEER	1200000	3	REJECTED
4	ASTROE_ASH	MANAGER	130000000	0	REJECTED
5	AMAZON_HIRE	BIG DATA ENGINEER	100000000	2	APPLY

Fig.3. Jobs Page

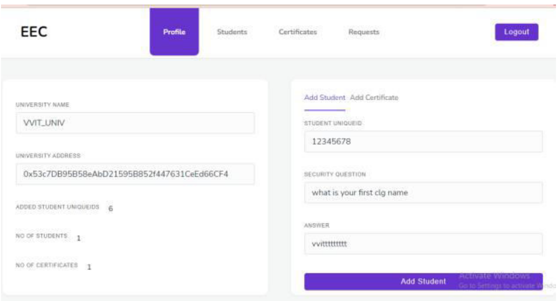


Index	Name	Job Name	Salary	No Of Applications	Status
0	VIRTUSA	Front end engineer	2500000	1	HIRED
1	VIRTUSA	DATA SCIENTIST	650000	0	Cancel
GANESH_1-1.jpg Cancel Pic			CERTIFICATE ID 9014870096		Apply
2	APPLEEE	BACK END	1000000	2	APPLY
3	ASTROE_ASH	DATA ENGINEER	1200000	3	REJECTED
4	ASTROE_ASH	MANAGER	130000000	0	REJECTED
5	AMAZON_HIRE	BIG DATA ENGINEER	100000000	2	APPLY

Fig.4. Apply for Jobs Page

University

The University after login using university name, can view their profile, can enter the student details like student unique id, and upload student certificates, accept the requests from company and send the certificate of the requested student.



UNIVERSITY NAME
VVIT_UNIV

UNIVERSITY ADDRESS
0x53c7DB95B58eAbD21595B852f447631CeEd66CF4

ADDED STUDENT UNIQUEIDS 6

NO OF STUDENTS 1

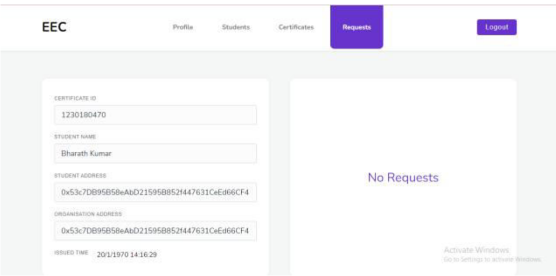
NO OF CERTIFICATES 1

STUDENT UNIQUEID
12345678

SECURITY QUESTION
what is your first clg name

ANSWER
vvittttttttt

Fig.5. Upload student details/certificates page



CERTIFICATE ID: 1230180470

STUDENT NAME: Bharath Kumar

STUDENT ADDRESS: 0x53c7DB95B58eAbD21595B852f447631CeEd66CF4

ORGANISATION ADDRESS: 0x53c7DB95B58eAbD21595B852f447631CeEd66CF4

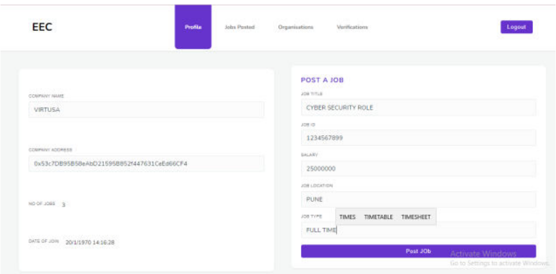
ISSUED TIME 20/1/1970 14:16:29

No Requests

Fig.6. Processing Requests Page

Company

The company can login using their company name. After login the company can view their profile and post jobs which include job title, job id, salary, type of job and location. The company can also view the jobs it posted and can also verify the students certificate if any student apply for jobs.



COMPANY NAME: VIRTUSA

COMPANY ADDRESS: 0x53c7DB95B58eAbD21595B852f447631CeEd66CF4

NO OF JOBS 3

DATE OF JOIN 20/1/1970 14:16:28

POST A JOB

JOB TITLE: CYBER SECURITY ROLE

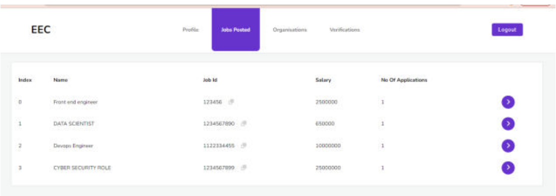
JOB ID: 1234567899

SALARY: 25000000

JOB LOCATION: PUNE

JOB TYPE: FULL TIME

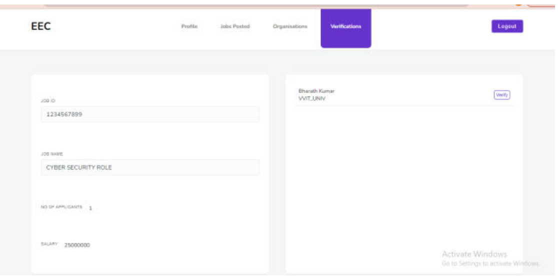
Fig.7. Post Jobs



Index	Name	Job Id	Salary	No Of Applications
0	Front end engineer	123456	2500000	1
1	DATA SCIENTIST	1234567890	650000	1
2	Devops Engineer	1122334455	10000000	1
3	CYBER SECURITY ROLE	1234567899	25000000	1

Fig.8. All jobs posted by company

After any student applied for specific job role the company can verify them by clicking the verify button.



JOB ID: 1234567899

JOB NAME: CYBER SECURITY ROLE

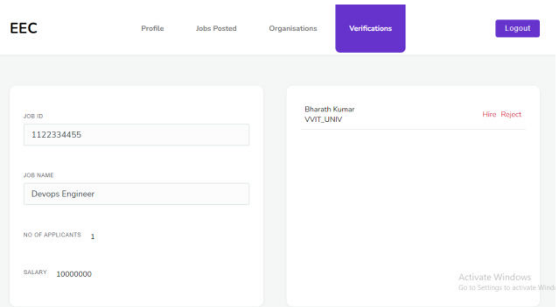
NO OF APPLICANTS 1

SALARY 25000000

Bharath Kumar
VVIT_UNIV

Fig.9. Company can verify by clicking on the verify button

If the students certificates hash values matches with the certificate provided by the college. Then the company can have two options Hire/Reject, else if the hash value does not matches then the company has only one option that is Reject.



JOB ID: 1122334455

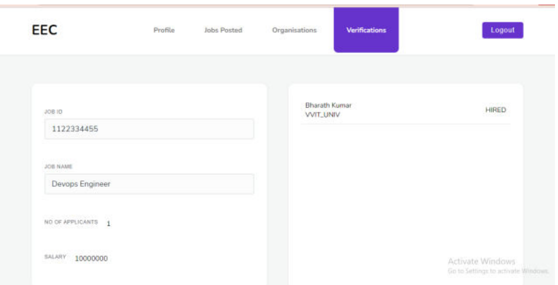
JOB NAME: Devops Engineer

NO OF APPLICANTS 1

SALARY 10000000

Bharath Kumar
VVIT_UNIV

Fig.10. HIRE/REJECT Page



JOB ID: 1122334455

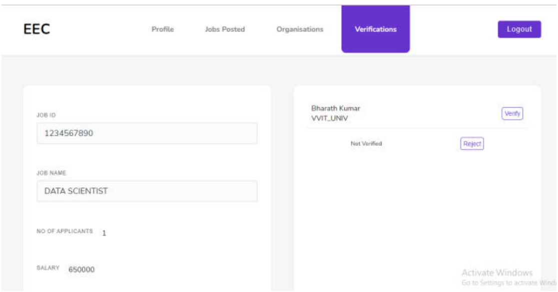
JOB NAME: Devops Engineer

NO OF APPLICANTS 1

SALARY 10000000

Bharath Kumar
VVIT_UNIV
HIRED

Fig.11.HIRE Page



JOB ID
1234567890

JOB NAME
DATA SCIENTIST

NO OF APPLICANTS 1

SALARY 650000

Bharath Kumar
VVIT_UNIV

Not Verified

Fig.12.REJECT Page

Conclusion

In conclusion, the integration of blockchain and cryptography in a digital certificate validation system provides an enhanced level of security and immutability to the verification process. By leveraging the cryptographic algorithms and hash functions, the proposed system can ensure that certificates are authentic and tamper-proof. The system provides transparency and trust in the verification process. The proposed system eliminates the need for centralized authorities, making the verification process faster and more efficient. The proposed system can be easily integrated into existing certificate verification processes, providing a seamless and reliable means of verification.

Future Scope

In future the proposed system can be expanded to other industries beyond education and employment, such as healthcare, finance, and government, where certificate validation is critical.The system can be enhanced with multi-factor authentication features such as biometric authentication, further increasing the security and reliability of the verification process.

References

[1] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen," An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE 6th International Congress on Big Data, 2017.

[2] Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, "Blockchain and Smart Contract for Digital Certificate," Proceedings of IEEE International Conference on Applied System Innovation 2018.

[3] Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Technology", International Journal of Recent Technology and Engineering (IJRTE), Volume-7, Issue-5S3, February 2019.

[4] Ravi Singh Lamkoti, Devdoot Maji, Hitesh Shetty, Bharati Gondhalekar, "Certificate Verification using Blockchain and Generation of Transcript", 2021, IJERT, ISSN: 2278-0181, Vol. 10 Issue 03, March-2021

[5] T Sai Charitha, Kandakatla Anirudh Baba, "A System for Academic Certificates Verification Using Blockchain", IJRASET, ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue VI June 2022.