IJCSE

Research Paper

Smart Transfer Certificate Generator and Employer Verification Using Blockchain

Shabina Sayyad-Modi[1]*(iD)**, Rashmi Kishor Shingate[2]**(iD)**, Rutuja Girish Jagtap[3]**(iD)**, Mayuri Dattatray Kadam[4]**(iD)**, Rutuja Hemant Sabale[5]**(iD)

[1,2,3,4,5]Dept. of CSE, Karmaveer Bhaurao Patil College of Engineering, Satara, DBATU, Lonare, India

Corresponding Author: shabina.sayyad@kbpcoes.edu.in

Abstract: Around 315 million students are enrolled in universities in India, which has the world's largest body. There are an enormous number of students who graduate each year with different degrees. In their education, they require various certificates, transcripts, degrees, diplomas, transfer certificates, etc., Due to the high number of graduate students, it can be difficult to establish whether an academic document is legitimate, and without any validating authority, it becomes even more challenging. To address this, we suggest using blockchain technology to create digital transfer certificates that are tamper-proof and will serve as a reliable form of authentication both in academic institutions and workplaces. Also, it will help the institute Tracking of these certificates and their verification manually becomes a hectic job and also the process will be handy for the students. Through the unique QR code of each document, certain authorities can easily verify the documents.

*Keywords***:** Blockchain, Digital certificate, Certificate Generation and Verification.

1. Introduction

India boasts the world's largest student population, encompassing approximately 315 million students. Each year, a significant number of students graduate with a wide range of degrees. Every time while changing the university or colleges students require a transfer certificate. It is a very hectic job to keep track of and verify certificates. These certificates are of importance while the admission procedure and while applying for jobs. As the various certificates are hard copies, they can be easily misused or forged. And as there is no such system to check whether the certificates are valid or invalid, in a populated country like India, some people are misusing and forging certificates on a large scale. On the other hand, if a student misplaces or loses his/her certificate or degree, the student has to apply to the institution for another copy of the document which takes a lot of time and effort. Meanwhile, there is no such central authority that generates or verifies the documents of the entire country, though it is a complex task but is of greater need.

Also, a candidate's journey ends once the offer letter has been rolled out, but a recruiter's journey is nowhere close to the finish line. So it is very important to validate the candidate's documents and details, sometimes reaching out to the college, and re-evaluating their decision is not possible or documents which are provided by candidates are invalid. In this case, companies have to bear huge losses. Traditionally HR of an organization mails the college authority to verify a particular student and colleges send the record of verification. Unfortunately, this process requires too much manual work and time.

So, this project will provide an anti-forge mechanism and eradicate the foul means of forging the certificates and create a collective database where all the information of the student such as college fees, certificates, marksheets, library dues, etc. are stored which will be used for verification. The verification system itself generates a digital transfer certificate with unmodifiable properties of the blockchain, which will enhance not only the credibility of various paper-based certificates but also reduces the risks of misuse of various certificates.

2. Literature Survey

A number of researchers have explored the use of blockchain to store university grades,university transcripts,a group at the University of Glasgow has developed a functional prototype for storage of student grades at the institution[1]. The platform chosen was ethereum, hence it was built on a public blockchain. This was exploratory research, and they identified several challenges, including in the use of smart contracts to calculate grades in an algorithmic manner[2]. Our proposed system utilizes Ethereum smart contracts and leverages the benefits of IPFS, to store the certificates in a decentralized file system.We intend to ensure confidentiality and validity of the certificates.So, to provide confidentiality,

the certificates will be encrypted with the AES algorithm before creating the transaction. On the other hand, validity is ensured by signing the transaction with the private key of the issuer university. the system offers a user-friendly interface, making it easier to access certificates, without the need to create a private wallet, or without even knowing what blockchain technology, with the introduction of a QR scanner, users will not even need to remember anything. With the use of optional features such as IPFS[3].

3. Proposed Methodology

A. Modules

1. Ethereum :
To use Ethereum for blockchain-based certificate verification, followed these general steps:

1. Certificate Creation: Certificates are generated and stored on the Ethereum blockchain using a smart contract. Each certificate is associated with a unique identifier and relevant metadata.
2. Publicly Accessible Data: Ensure that the certificate information you want to verify is publicly accessible.
3. Certificate Retrieval: Obtain the certificate identifier or any other necessary information from the entity presenting the certificate for verification.
4. Accessing the Ethereum Blockchain: Interact with the Ethereum blockchain using a tool or programming language that supports Ethereum, such as web3.js.
5. Querying the Smart Contract: Use the certificate identifier or relevant information to query the smart contract on the Ethereum blockchain.
6. Verify Certificate Authenticity: Once you receive the certificate details from the smart contract, you can compare them with the presented certificate to verify its authenticity. Ensure that the metadata matches, including the recipient's name, issuing organization, date of issuance, and any other relevant information.
7. Trust in Blockchain Immutability: By leveraging the decentralized nature of the Ethereum blockchain, you can trust that the certificate's information cannot be tampered with or modified without leaving a trace.

2. Blockchain :
By leveraging the unique features of blockchain technology, such as immutability, decentralization, transparency, and security, blockchain-based certificate verification ensures trust, efficiency, and integrity in the verification process, bringing benefits to both issuers and recipients of certificates.

3. Smart Contract :
Smart contracts enable automated, decentralized, and tamper-proof verification of certificates on the blockchain, ensuring transparency, efficiency, and trust.

4. Solidity :
Solidity allows developers to write the code for smart contracts that define the rules and logic for verifying certificates. Solidity enables the storage and management of certificate metadata on the blockchainSolidity provides the flexibility to define the logic for certificate verification within smart contracts. Supports access control mechanisms, allowing developers to define permissions and roles for different entities involved in the certificate verification system

5. IPFS :
IPFS is an "InterPlanetary File System".IPFS can be used to store the certificate files, including any supporting documents or evidence associated with the certificate. Each certificate file is given a unique content identifier (CID), which serves as its address on the IPFS network. Once a file is uploaded to IPFS, it receives a unique CID that is generated based on the content's hash. Any modification to the file content will result in a different CID, making it evident that the file has been tampered with.

6. Metamask:
Metamask provides a user-friendly interface for managing cryptocurrency wallets, specifically Ethereum wallets. Users can install Metamask as a browser extension and create or import Ethereum wallets to securely store their digital assets, including certificates or certificate-related tokens. Metamask enables users to sign transactions securely.

7. Ganache :
It's specifically designed for Ethereum developers. Developers can set up and run Ganache on their local machines, allowing them to develop and test their certificate verification system in a controlled environment without interacting with the live Ethereum network. Developers can use this interface to test and debug their certificate verification system, inspect transaction details, and track contract interactions in real time.

8. Truffle :
Developers can write the smart contracts responsible for certificate verification using the Solidity programming language within Truffle projects. Truffle also offers built-in libraries and utilities that assist in writing, compiling, and deploying smart contracts.

9. Node JS :
In the context of a certificate verification system, Node.js can be used to build the backend infrastructure that interacts with the blockchain network and handles certificate verification requests from clients.

10. Digital Signature :
The digital signature is computed by applying a cryptographic algorithm to the certificate's data, creating a unique and verifiable representation of the certificate. This ensures that only the issuer with the corresponding private key could have produced the signature, establishing the authenticity of the certificate

B. Project Description
To overcome the current system, we have proposed a system that will automatically generate transfer certificates and also validates them. The data will be reliable, authenticated, and trustworthy.
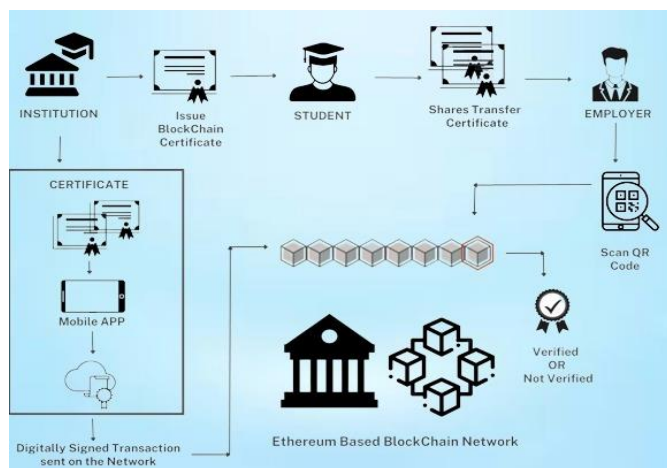

Fig.1. Workflow of the System

System Design and Working

Through the proposed methodology we can determine whether a document is valid or not and also check the originality, integrity, and trustworthiness with the help of distributed technologies like Ethereum smart contracts and IPFS. How users engage with smart contracts is depicted in the above diagram.

a) College: Colleges issue the authorized certificate through the blockchain platform and also validate the students. It acts as a middleman between students and employer

b) Student: The student can do payments through the platform. After the validation through college, students can download their unique transfer certificates as well as QR code which have lifetime access

c) Company: Through the platform, the employer can check the integrity and authenticity of the documents.

Following the college's upload, the document's information is first collected and stored in IPFS which will generate a unique hash for every document. IPFS sends this information to the Blockchain. Now, the generation charges in Metamask must be approved by the issuer. This hash is then saved in the Blockchain and cannot be modified later. Students can send QR codes along with the document to the employer and the employer can able to verify through the blockchain

4. Implementation Details

Fig.2. Use Case

The key components of the project are undergraduates, colleges, and employers. Initially, the authority registers pupils on the portal, establishing their sketches in addition to academic news. To get a transfer authentication, undergraduates must settle all imminent payments. Once all liabilities are emptied, the request for a transfer authorization is accessible to the graduates.

The smart contract serves as the center for Ethereum blockchain. Remix, an Ethereum IDE, is taken advantage of to evolve, kill, and redistribute smart contracts utilizing Solidity. We have worked on Remix to run Solidity on smart contracts.

After document transfer, bureaucracy produces a mess of the document when presented to a peace sender. The mix-up is conceived utilizing the SHA-255 invention. Simultaneously, while the document is being uploaded to IPFS (InterPlanetary File System), an attempt is created to transfer data to a server the document mess to the blockchain. Confirmation of the undertaking is anticipated, and before habitual, the next step search out guarantees addition in the blockchain. Thus, the document's mix-up is stocked on the blockchain while the document itself is stocked in IPFS. Successful finishing of these steps means the favorable transfer of data to a server of a document. The pursuing pupil accepts a QR rule defining the mess of their document, in addition to the document file.

When a grading undergraduate wishes to authorize a course or chase further studies, they can comply with either the document file or the QR law supported by their basic academy to the wanted association or academy. The engaged institution then visits the principal academy's site to validate the genuineness of the pupil and check for some counterfeiting. The institution uploads the undergraduate's document file (or employs the QR rule) to the academy's person studying at the institution of higher education document proof page. The system hashes the document to equate it accompanying the hashes then stocked in the blockchain for one issuer. If the document's mix-up supported apiece graduate is in the direction of the blockchain, the next step includes achieving the document itself from IPFS to further enact allure believableness. The document verification process is deliberately profitable if all these steps are joined. Conversely, if the graduate is a falsifier or does not maintain a strength from the academy, the proof will forsake. Employers will come together if the scholar confirms a suggestion of correction.

This process is occur flatly, securely likewise dossier safety and privacy is attained utilizing peer to peer blockchain

5. Advantages

1. Reduce staff work and time involved in the manual verification process.
2. Need not to carry paper certificates and have fear of loss or tampering.

3. No one can view documents except issuers and document holders.
4. Complete Data Privacy.
5. Free from any central point of failure Impossible to fake your certificates.
6. No risk of forged certificate claims.

6. Applications

1. Certificates are securely stored on Blockchain Network.
2. Issues related to fake certificates will be avoided.
3. Certificates are easily accessible
4. Manual Verification of the Certificate takes more time. This issue will be solved

Conflict of Interest
We don't have any conflict of interest.

Author's contribution
All authors are involved in the completion of the project . The final version of the manuscript was authorized by all authors.

Acknowledgment
We would like to thank Dr.Shabina Sayyad for feedback and suggestions which will help us to improve the quality of this paper.

7. Conclusion

Our system will automatically generate transfer certificates for students, eliminating the need for them to carry physical certificates and reducing the risk of loss or tampering. With just one click, students can apply for their certificates and they need not to run from one section to another for approval. Additionally, the student data will be kept completely secured. This efficient process will greatly benefit College, saving valuable work and time that would otherwise be involved in manual verification processes. Within a single click, the employer will get to know if the student is verified or not and also reduce cost on third-party background verification for certificate authenticity and reduced time for employee verification. Implementing this system will streamline the certificate generation process, enhance security, and significantly reduce manual work.

References

[1].J. Rooksby and K. Dimitrov, "Trustless education? A blockchain system for university grades," New Value Transactions Understanding and Designing for Distributed Autonomous Organizations Workshop at DIS 2017, **2017.**
[2].T. Arndt, "Empowering university students with blockchain-based transcripts," in Proc.CELDA 2018, Budapest, Hungary, October, pp.**21-23, 2018**
[3].Development and Evaluation of Blockchain based Secure Application for Verification and Validation of Academic Certificates.Elva Leka1,2,* and Besnik Selimi1, Annals of Emerging Technologies in Computing (AETiC) Vol. 5, No. 2, **2021**