Blockchain Based Certificate Generation and Validation

Omraj Jadhav   
*Department of Computer Science and Engineering*  
*Karmaveer Bhaurao Patil College of Engineering*Satara, India  
omrajjadhav07@gmail.com

Prasenjit Bhosale  
*Department of Computer Science and Engineering*  
*Karmaveer Bhaurao Patil College of Engineering*Satara, India  
prasenjitbhosale111@gmail.com Aniket Chavan  
*Department of Computer Science and Engineering*  
*Karmaveer Bhaurao Patil College of Engineering*Satara, India  
chavananiket1272@gmail.com

Akshata Dhumal  
*Department of Computer Science and Engineering*  
*Karmaveer Bhaurao Patil College of Engineering*Satara, India  
akshata.dhumal792@gmail.com Akhilesh Dange  
*Department of Computer Science and Engineering*  
*Karmaveer Bhaurao Patil College of Engineering*Satara, India  
akhileshdange47@gmail.com

Yashshri Deshmukh  
*Department of Computer Science and Engineering*  
*Karmaveer Bhaurao Patil College of Engineering*Satara, India  
yashshri.deshmukh01@gmail.com

*Abstract*

Statistics from the Indian Ministry of Education indicate that document verification is a difficult field with many obstacles and time-consuming procedures involved in document authentication. When there are insufficient anti-forgery safeguards in place, instances of falsified graduation certificates are frequently discovered. We support the implementation of a digital certificate system based on blockchain technology in order to address the issue of fake certificates. The most significant documents that institutions provide to their pupils are their educational certificates. Nevertheless, due to the lack of transparency and verifiability in the issuing process, it is relatively easy to create counterfeit certifications. Fake certificates that are expertly created can be difficult to spot and may even be identical to real ones. Document forgery damages the credibility of the entity that issued the document as well as the person in control of it. In order to tackle the issue of certificate forgeries, we recommend putting in place a blockchain-based digital certificate system. Utilizing the immutability of blockchain technology, digital certificates can be issued with embedded verifiability and anti-counterfeit features. The process of issuing digital certificates within this system involves several steps: Initially, an electronic file of a paper certificate is generated and stored in the database, along with pertinent details. Simultaneously, the hash value of the electronic file is computed. Subsequently, this hash value is retained within the blockchain system. The objective of this research is for the authors to pinpoint the critical security elements necessary for blockchain-based document verification. Additionally, the study sheds light on the deficiencies and vulnerabilities in the current state of blockchain-based educational certificate verification system. The system will generate a unique inquiry string code and a corresponding QR code for the paper certificate. This enables the recipient to authenticate the paper certificate either through online queries or by scanning it with a mobile phone. This will empower individuals making requests to verify the authenticity of paper certificates either by scanning them with a mobile phone or by conducting online inquiries.

Keywords— Blockchain, Ethereum, Smart Contracts, Security, Certificate Generation

# Introduction

Maharashtra had gone through some waver last year as to the retail cost of oranges. The cost jumped from Rs. 26 for each kilo in the early portion of the year to an astonishing Rs. 50 for every kilo in August. Observing the rise in the price, many of the farmers in the state to cultivate oranges on their farm, in hope of making, The widespread use of mobile phones and tablets, widespread access to the Internet, and improvements in information technology have totally transformed how people live. Digital cookies, or digital funds, were first created for use online but are now being widely used offline. Several digital currencies, including the popular ones like Bitcoin, Ether, and Ripple, are witnessing a surge in popularity owing to the widespread accessibility of the Internet. Indeed, the value of these currencies has seen a recent uptick. The fundamental technology behind these innovative currencies, blockchain, is beginning to catch the eye of the public. Blockchain boasts a decentralized, immutable ledger that holds promise for a variety of applications.. Blockchain is a widely used distributed database for recording a wide range of transactions. Once a consensus is achieved among different nodes, the transaction is appended to a block containing records of multiple transactions. To create a connection, each block includes the hash value of the block before it. Blockchain is a type of decentralized database that is often used to protect transactions. Data are decentralized as they flow through multiple nodes, or dispersed data storage. Consequently, these nodes work together to uphold the database. A block within a blockchain is deemed validated only upon confirmation by numerous parties. Moreover, altering the data within blocks arbitrarily is not feasible. For instance, a blockchain-based smart contract establishes a reliable system by dispelling doubts about the accuracy of information.

# Literature Review

## Blockchain and Smart Contract for Digital Certificates:

As per data from the Taiwan Ministry of Education, around one million students graduate annually, with some opting for further education abroad, in high schools, or tertiary institutions, while others prepare for employment or seek job placements. During the course of schooling, students' achievements such as conduct awards, academic transcripts, diplomas, etc., become crucial references for admission to new schools or careers. When schools issue different honours or diplomas, usually only the names of the schools and students are documented. When schools administer sundry accolades or diplomas, merely the designations of schools and pupils are recorded. Because there isn't a strong anti-forgoing system in place, stories regarding graduation certificate fraud frequently surface. To address the issue of counterfeit certificates, the blockchain-based digital certificate system is put forth. The unchangeable nature of blockchain facilitates the creation of digital certificates with verification and anti-counterfeit capabilities. In such a setup, the procedure for distributing digital certificates proceeds as follows: Firstly, while computing the hash value for this electronic record, an electronic record of the paper certificate is stored in the database along with any relevant additional data. Subsequently, this hash value is inserted into a blockchain block for safekeeping. The system generates both a QR code and a query sequence code that can be attached to the paper certificate. This will enable the recipient to verify the authenticity of the paper certificate through mobile phone scanning or online queries. It shall furnish the requesting entity with the capability to authenticate the legitimacy of the paper certificate via mobile phone scanning or website interrogations. Due to the immutable characteristics of blockchain, the system not only enhances the trustworthiness of numerous paper-based certificates but also digitally minimizes the risk of various certificate losses.

## Certificate Transparency and Revocation Transparency Using Blockchain:

In traditional X.509 public key infrastructures (PKIs), the signature of certificates, crucial for authenticating web servers and establishing secure channels in SSL/TLS, relies on trustworthy certifying authorities (CAs). Recent security incidents have raised concerns about the potential compromise of Certificate Authorities (CAs) for signing fraudulent certificates. In this work, we offer a blockchain-based approach to address this problem by providing Certificate Transparency (CT) and Revocation Transparency (RT). Even with X.509 PKI compatibility, our approach greatly improves certificate security. Using this method, CA-signed certificates and information about their revocation status are released by the subject or web server as transactions on the global certificate blockchain. The certificate blockchain, which serves as append-only public logs to track the certificate signing and revocation activities of CAs, offers cooperative control over the certificates of an SSL/TLS web server. A browser will only accept a certificate in the SSL/TLS negotiation procedure if it has been officially issued, made public, and is still valid after cross-referencing it with the certificates kept on the public blockchain. Our development work with Nginx and Firefox for creating the prototype system has shown that it incurs only minor overhead. The security of web communication using SSD/TIS protocols depends on the secure distribution of public keys linked to web domains through X.509 certificates. This includes using Certificate Transparency in conjunction with Blockchain, which ensures the safe sharing of public keys linked to online domains using X.509 certificates, resulting in boosting the security of web communication in SSD/TIS protocols.

## Certificate Transparency Using Blockchain:

The secure distribution of public keys connected to online domains in the form of X.509 certificates is essential to the security of web communication through the SSD/TIS protocols. A browser will only accept a certificate in SSL/TLS discussions if it has been published and is unrevoked, comparing it to those kept in the public certificate blockchain. The trial findings indicate that the prototype system, which is developed with Nginx and Firefox, adds manageable overheads. C. Blockchain Technology for Transparent Certificates: In the realm of transparent certificates using blockchain technology, the secure distribution of public keys associated with web domains via X.509 certificates are crucial for ensuring the security of web communication under SSD/TIS protocols. Within CTB, we are working hard to set up a mechanism for revocation of certificates. In order to build CTB, our strategy makes use of IBM's Hyperledger Fabric blockchain technology. The Go-coded CTB smart contract is accessible for thorough review.

## Blockchain-Based Decentralized System for Certificate Revocation::

Existing approaches to revoking digital certificates prove inadequate in scenarios involving multiple certification authorities (CAs), resulting in a deficiency of mutual trust, access reliability, and timely data synchronization among CAs. We propose a decentralized approach to digital certificate cancellation using a combination of secret-sharing and consortium blockchain technologies. In certain cases, this method may render the digital certificate ineffective, safeguarding user information and property security. Consortium blockchain technology, which takes advantage of decentralized consensus processes, is the core of the system. Once this system successfully enables collaborative management of digital certificate revocation lists (CRLs) across multiple Certificate Authorities (CAs) and incorporates a secret sharing scheme, it could lead to the creation of an Online Certificate Status Protocol (OCSP). This advancement increases the maintenance process's reliability and makes the system safer, resilient, and resistant. Unlike traditional revocation methods, this innovative solution creates a robust and credible Certificate Revocation List (CRL) system that is shared by several certification authorities (CAs). A system like this could open up new perspectives on the revocation of digital certificates and expand the range of uses for blockchain technology.

## Certificate Verification System using Blockchain:

For quite some time, there has been a significant issue with the proliferation of fraudulent certificates. The drive for individuals to secure employment has led to the commercialization of certificate issuance.. Since the holders of these phony credentials deny them what may be theirs, hardworking individuals with valid degrees or certifications must bear the repercussions of this phenomena. This may often prove to be quite harmful. Imagine a situation in which a surgeon performs surgery based only on a fake degree. Such incidents highlight how crucial it is to have a system that can authenticate and validate certificates, as well as the holders and issuers of them. In this paper, we present a methodology that takes benefit of the tamper-proof and non-repudiation properties offered by blockchain technology to facilitate the issuance and validation of certificates.

# Methodology

## Issuing User Certificates:

Through the Ethereum network, users can get their certifications from the colleges or government agencies that belong to their respective institutions.

## Digital Lockers and Blockchain Storage:

For ensuring immutability and security, each user possesses a digital locker on the Ethereum blockchain, where they can securely store their certificates using smart contracts.

## Unique Certificate Identifier:

As a safe identification, every certificate has a distinct hash number linked to it.

## Generate Unique URL/QR Code:

Every certificate has an automatically produced unique URL or QR code that points to the blockchain-stored certificate.

## Share Certificates: Users send the created QR code or URL to businesses and others who ask for verification.

## Organization Verification:

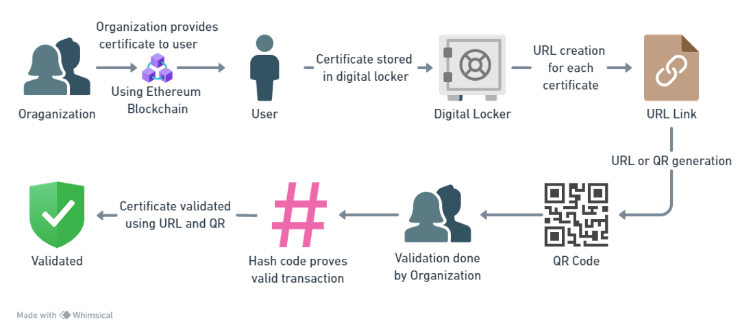
Organizations visit the website and start the authentication process by using the URL or QR code that the user provides.

## Validation:

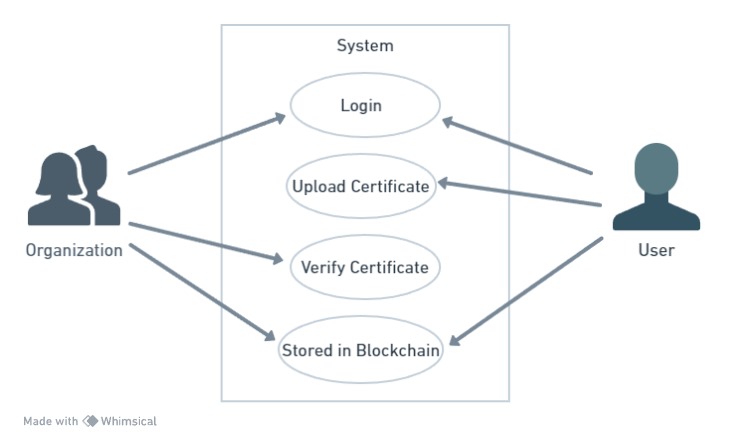
The validation procedure guarantees the certificate's legitimacy. Through the verification of blockchain data linked to the supplied URL or QR code, the system authenticates certificates.

## Record Keeping and Inspection:

Transparency and security are maintained by recording all certificate-related transactions on the Ethereum blockchain, encompassing both creation and validation processes.



A distributed, decentralized database is what blockchain is. The following are the procedures by which the system created in this study operates: Schools offer degree certificates in addition to submitting the student's data into the system. The student's serial number is then immediately logged onto a blockchain by the technology. The certificate system verifies all of the data. Instead of typical paper copies, schools award e-certificates with a rapid response (QR) code to graduates whose data has been properly authenticated. Every graduate also receives an inquiry number and an electronic file for their certificate. When seeking for a job, a graduate only needs to email the target firms their e-certificate with a QR code or their serial number. When businesses reach out to the system wfoith inquiries, it lets them know if the serial numbers are authentic. The QR code lets them to check whether the certificate has been tampered with or is fraudulent.

  
The system suggested utilizing its own private blockchain to create dynamic certificates in a novel way. The first step is for the student to apply online for an e-certificate and submit all of their academic records. Web portal is an accredited, reliable third party that verifies all university, college, and school paperwork, among others. The technology creates a unique certificate ID or QR code, stores the data on a blockchain, and sends the data back to the student following a successful verification process conducted by a university, college, or school. Students can give the organization their certificate ID or assigned QR code in place of sending hard copies of the paperwork. Through the site, organizations can gather the associated student's e-certificates, authenticate them, and upload their IDs or QR codes.  
We created a smart contract on the blockchain to streamline the entire process. We conducted tests to assess the proposed system's resistance against different types of network assaults, including Man-in-the-Middle (MiM) and Denial-of-Service (DoS) attacks, as well as to test it in a susceptible setting. For every student's paper, the suggested method creates a distinct certificate and dynamic QR code. Data e-certificates that are securely held on the blockchain increase security. The smart contract technology permits modifications throughout the blockchain, according to this as well. This research recommended a custom blockchain development using an open-source framework.

# Preliminary Data

## Existing System:

Nowadays, everyone chooses to pursue education in order to land a decent career. In order to do this, individuals are creating phony diplomas, which cannot be verified by current technologies.

*Drawbacks of the Current System: Lack of assistance for certificate verification*

## Proposed System:

Therefore, we are presenting blockchain technology in our proposed paper, which stores immutable data that cannot be altered in any way. Therefore, upon storing a copy of the certificate on the blockchain and retrieving it, the administrative user will generate a QR code using the certificate's digital signature and attach it to the student's certificate. This certificate can be scanned by other companies or organizations to verify and retrieve data from Blockchain. If QRCODE is included in the blockchain, then the certificate validation procedure will be successful.

## Advantages of proposed system:

The possibility of certificate forgery is decreased by the suggested blockchain-based solution. The automated certificate issue process in the system is open and transparent, as is the certificate application process.

## FUNCTIONAL REQUIREMENTS

1. Modeling

2.Data Preprocessing

3. Predicting

4.Data Collection

5.Training and Testing

## NON FUNCTIONAL REQUIREMENTS

Non-functional requirements (NFRs) outline a software system's quality attributes. They evaluate the software system based on non-functional criteria like usability, security, portability, and responsiveness that are essential to its success. An example of a nonfunctional need might be "how quickly can I load the website?" Systems that don't fulfill user demands might be the consequence of not meeting non-functional criteria. Non-functional requirements provide you the ability to place limitations or limits on how the system is designed across different iterations of the agile backlog. For instance, the website should load in three seconds if there are more than 10,000 people registered in at the same time. It is equally important to describe non-functional needs as it is to outline functional requirements.

* Scalability requirement
* Availability requirement
* Usability requirement
* Capacity requirement
* Interoperability requirement
* Security requirement
* Environmental requirement
* Reliability requirement
* Maintainability requirement
* Regulatory requirement
* Manageability requirement
* Recoverability requirement
* Serviceability requirement
* Data Integrity requirement

# Discussion

## Blockchain Technology :

Blockchain is a database where multiple users have the capability to add, modify, and remove entries. Since it only offers the ability to add data, once input, it cannot be altered or withdrawn; it is immutable. Hashing: A message digest, also known as a hash value or hash, is a number that is produced from a text string. Security systems use hashes to make sure that messages haven't been tampered with during transmission. The block's prior hash value is always the same as the hash value of the preceding block. Scientists Stuart Haber and W. Scott Stornetta first presented blockchain concept in 1991. To prevent retroactive alterations and manipulation, their objective was to introduce a computationally viable method for timestamping digital documents. Since 1995, the New York Times has featured the oldest and longest blockchain in the world. Three types of blockchain exist: I) Public Blockchain, which includes Ethereum, Bitcoin, and other similar platforms. II) Hyperledger and R3 Corda make up the private blockchain. III) The Dragon chain makes up the Hybrid Blockchain.

## Smart Contracts:

Smart contracts, or self-executing contracts, expressly incorporate the terms of the agreement into the code. Running on blockchain platforms such as Ethereum, smart contracts automatically execute and enforce the terms of an agreement once predefined conditions are met. Due to their tamper-proof, secure, and decentralized nature, smart contracts are revolutionizing various industries, including finance, supply chain management, and legal procedures.

## Advantages of the Proposed System- :

Self-executing contracts known as "smart contracts" are made up of explicit contract provisions encoded into the code. They operate on blockchain systems, like Ethereum, and when certain criteria are satisfied, they automatically carry out and enforce the terms and conditions of an agreement. Smart contracts are a game-changing invention in a number of industries, including supply chain management, legal procedures, and banking, since they are tamper-proof, safe, and decentralized.

### Modern and Relevant: Current project maintains the currency and value of certificates in current digital age. It is in line with contemporary procedures.

### Certificates Can't Be Altered: Certificates cannot be altered or falsified once they are stored on the blockchain. This guarantees that certifications are always authentic.

### Saves Money: Due to the reduction in the amount of resources required for paperwork and manual checks, businesses and schools can save money. This could result in substantial savings over time.

### Faster Certificate Issuance: Certificate issuance may be done directly on the blockchain by businesses and universities, eliminating the need for documentation. This expedites the certification process.

### Transparency and Trust: Secure records are kept of every step of the certificate creation and verification process. This maintains accountability and fosters trust.

### Easy Verification: Individuals can use specific URLs or QR codes to rapidly verify whether certificates are authentic. It's simple and quick.

### Reliable Validation: Our technology makes it easier for companies to distinguish between genuine and false certificates by providing a uniform and reliable method of certificate checking.

### User-Friendly: We have made our system user-friendly for everyone. It will be easy and clear for people who have credentials and those who verify them.

### Better Security: Our solution makes use of blockchain technology, which is incredibly secure and nearly impossible to hack. This shows that certificates are safe against manipulation and illicit use.

## Statement of Limitation - :

### Needs Internet: Our technology distributes and verifies certificates via the internet. But if you're in a place where internet connectivity is inconsistent or nonexistent, it may cause problems.

### Initial Setup Is Tricky: The system's initial setup, the development of smart contracts, and the integration of the system with other systems can be challenging and time-consuming.

# Implementation

Nowadays, everyone chooses to pursue education in order to land a decent career. In order to do this, individuals are creating phony diplomas, which cannot be verified by current technologies. Therefore, we are presenting blockchain technology in our proposed paper, which stores immutable data that cannot be altered in any way. Therefore, the admin user will create a QR code based on the digital signature on the certificate and attach it to the student's certificate after storing a copy of the certificate in the blockchain and obtaining it. Other businesses or organizations can scan this certificate to confirm and retrieve information from Blockchain. The certificate validation process will be successful if QRCODE is present in the blockchain.  
  
A distributed data storage system called blockchain makes it feasible to verify data using hash codes. It creates a peer-to-peer network in which several peers duplicate the data kept in a single peer. Within the blockchain, every data block is represented by a distinct hash code. Blockchain verifies previous hash codes before saving new records. If all hash codes match across nodes, new records are stored; if not, the data is deemed tampered with. As a result, blockchain data is difficult for third parties to alter, which is why it is called immutable.

This project, which consists of three modules, adds a certificate verification method utilizing blockchain technology to prevent certificate forgeries.

### Company: A company user only has to register and log in to the system. After that, they may upload and scan their certificate, which will be compared to digital signatures stored in the Blockchain by the program. If the digital signature issued by the application matches the original certificate, authentication will be successful.

### Admin: The admin, acting as an educational authority, accesses the system with the username "admin" and password "admin." Upon login, the administrator proceeds to upload the student's information and certificate to the blockchain. Each certificate has a distinct hash code that serves as a digital signature. Furthermore, this hash code is utilized to create a QR code that is linked to the student's certificate. Scanning this QR code with a smartphone allows retrieval of information from the blockchain. Confirmation of successful validation of the certificate is obtained if the QR code is found within the blockchain.

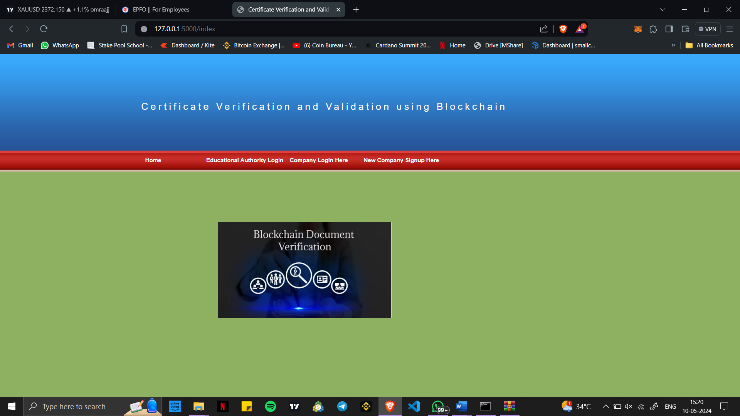
### Scanner Module: Education institutions and businesses will maintain this stand-alone module, which allows users to scan a QRCODE to take information from the blockchain.

By double-clicking the "run.bat" file, the Python server will launch and the output will be visible as seen below.

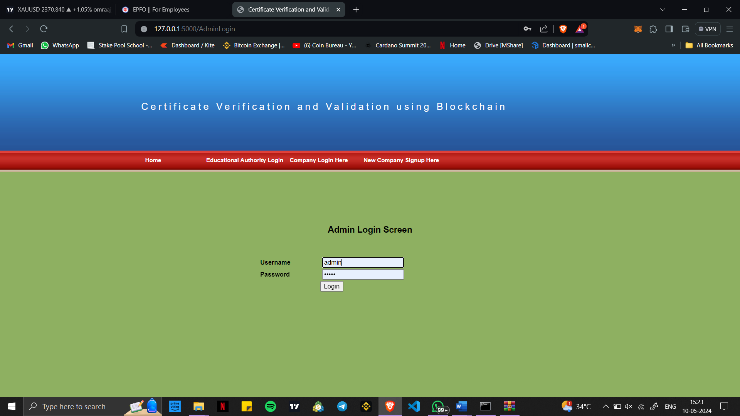
A screen shot of a computer program

Description automatically generated

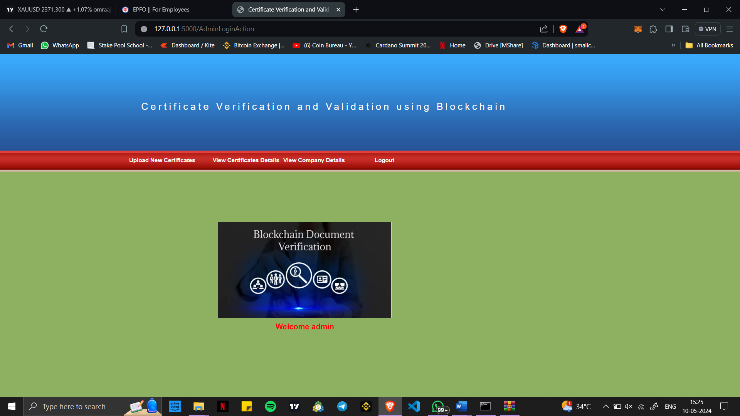
The screen above indicates that the Flask server for Python has begun to run. Open a browser, input http://127.0.0.1:5000/index, and hit Enter to display the page below.



Click the "Educational Authority Login" link in the upper screen to view the login screen below.



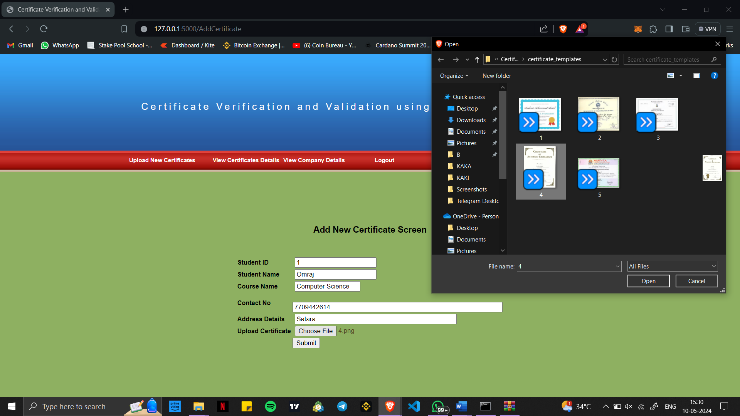
Upon logging in, the administrator will be presented with the screen below.



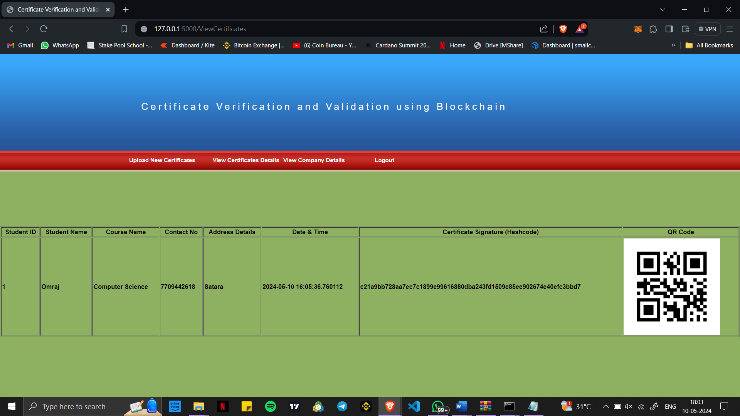
To upload a certificate, the administrator can click the "Upload New Certificates" option in the above screen.

. A screenshot of a computer

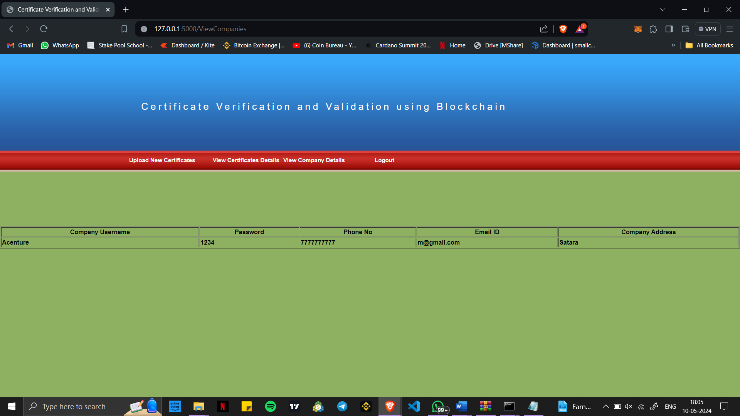
Description automatically generated



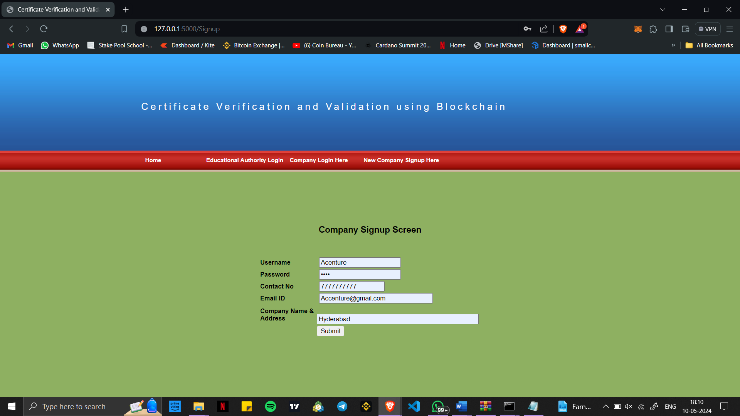
The administrator is entering student information on the screen above, uploading the certificate, and clicking "Submit" to produce the result below.



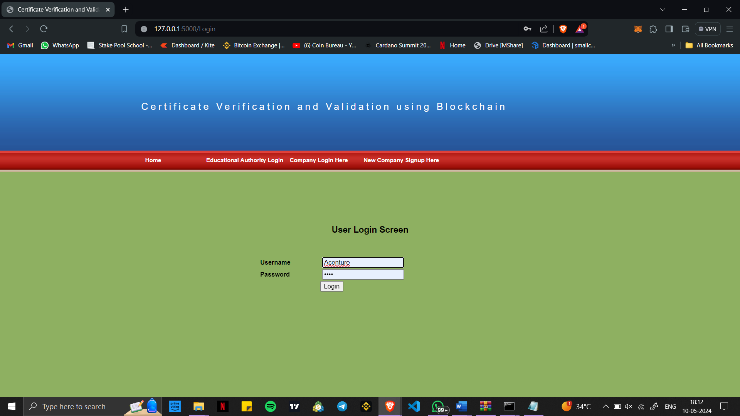
The screen that is displayed shows several credentials that are kept in the blockchain and can be attributed to various students or the same ones. Along with a digital signature and a QR code image, it also displays information like the upload date and time. Administrators can click on a QR CODE image to view registered companies. Admins can also click "View Companies Details" to view registered firms.



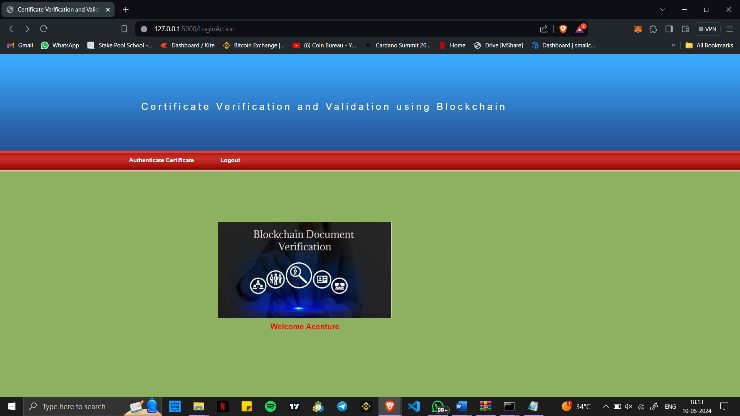
The administrator may see a list of registered firms on the page above. Log out and register a new company to complete the verification process.



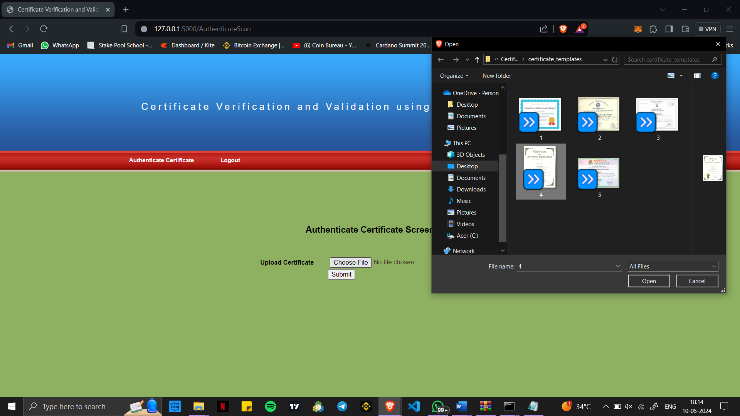
The company can enter registration details using the interface above. When the button is pressed, the information is entered into the blockchain, and the outcome is shown below.



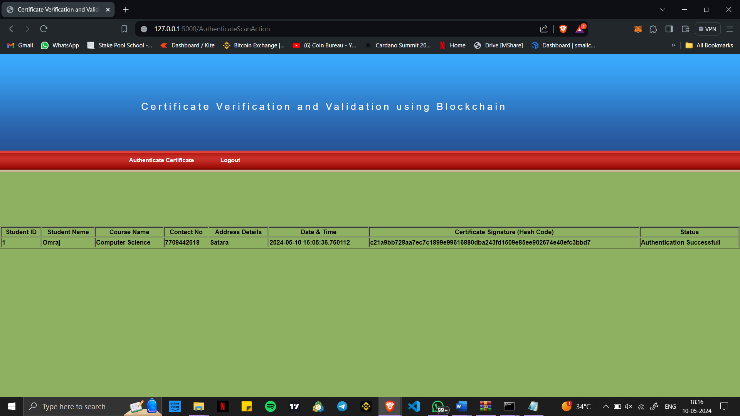
The corporate login screen is above, and the screen below appears after login.



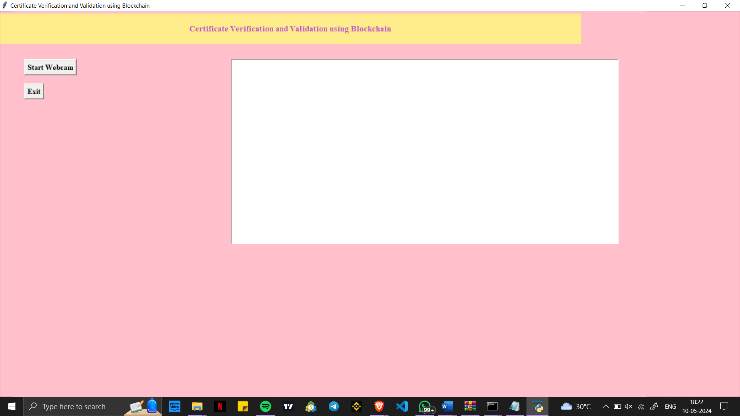
The company has the option to upload a duplicate of the student's certificate and begin the verification process by activating the "Authenticate Certificate" button shown on the screen above. Similarly, the firm can execute the verification procedure by uploading the student's certificate copy and selecting the "Authenticate Certificate" button displayed on the above screen.



If verified, the firm can upload a certificate on the top screen and receive the details below.



The firm may examine all uploaded certificate data in the screen above. Authentication success is shown in the last column. The company can also upload and validate any certificate.   
To validate certificates, businesses and educational institutions can scan QR codes. To do so, double-click the "RunWebCam.bat" file, which will yield the result shown below.

  
 To activate the camera and view the output below, simply click the "Start Webcam" button located at the top of the screen.

A hand holding a phone with a qr code on it

Description automatically generated

As soon as the QR code is displayed on the above screen, the Blockchain is consulted to extract all relevant information, which is subsequently displayed in the TEXT section above. Similarly, the output below will appear if we scan the incorrect CODE.

# Conclusion

Data security stands as a fundamental aspect of blockchain technology. The blockchain acts as an extensive, open-access online ledger in which every node stores and verifies the same data. The proposed blockchain-based method significantly decreases the likelihood of certificate forgery. Moreover, the system's automated certificate issuance and application processes ensure transparency and openness. Thus, companies or groups are able to ask the system questions respecting any certificate. To sum up, the information is precise and private thanks to the system.

# References

1. **"Blockchain Technology: Principles and Applications"** by Marc Pilkington, which is a part of the Research Handbook on Digital Transformations edited by F. Xavier Olleros and Majlinda Zhegu, the author gives a detailed overview of blockchain technology and its applications. This includes conversations on certificate creation and validation.
2. **"Blockchain in Education: Introduction and Critical Review of the State of the Art"** by Alexander Grech and Andréia Inamorato dos Santos, published in Publications, MDPI. This paper explores diverse applications of blockchain technology in education, encompassing certificate issuance and verification among others.
3. **"Towards Blockchain-based Digital Certificates for Learning: Technical Issues and Future Directions"** by H. Drachsler, D. Bogers, M. Vuorikari, and S. Kalz, published in the International Journal of Educational Technology in Higher Education, the authors delve into the technical aspects and hurdles involved in deploying blockchain-based digital certificates within the realm of learning.
4. **"Blockcerts: An Open Infrastructure for Academic Credentials on the Blockchain"** authored by M. Sporny, D. Longley, and M. Allen, appears in IEEE Security & Privacy. This paper introduces Blockcerts, an open standard designed for blockchain-based digital certificates, detailing its implementation and exploring potential applications.
5. **"Blockchain Solutions for Credentials and Certificates: Examples and Challenges from the European Perspective"** by Pauline van Mourik, published in European Journal of Education. This paper discusses examples of blockchain solutions for credentials and certificates in Europe and examines the challenges associated with their implementation.
6. **"Designing Blockchain-Based Systems for Secure and Trustworthy Credentials"** published in IEEE Transactions on Dependable and Secure Computing by K. Ren, A. Yu, X. Wang, and W. Lou. The architecture for developing blockchain-based systems for reliable and safe credentials, that involve certificate creation and validation, is presented in this paper.