



Decentralized Certificate Validation System Using Blockchain

Ms. K. Shirisha¹, Amena Arman²

¹Assistant Professor, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Gandipet, Hyderabad.

²Student, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Gandipet, Hyderabad.

ABSTRACT:

Traditional paper certificates and electronic certificates have difficulties in preservation and management, and other problems concerning inconvenient verification, poor reliability, anti-counterfeiting and anti-tampering. A decentralized certificate system is to be built that is based on blockchain technology, in which a set of blockchain certificate system aiming at providing blockchain certificate services. In this system, the process initiates by generating the electronic file of a paper certificate alongside other pertinent data into the database, simultaneously computing the hash value for the electronic file. Finally, store the hash value into the block in the chain system. The system will create a related QR-code and inquiry string code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning. Recruiters benefit from instant verification, streamlining the hiring process. This approach ensures certificate security through encryption while leveraging the transparency of the Blockchain for efficient verification by students and recruiters, offering a more secure and efficient digital certificate validation system.

Keywords: Blockchain certificates, decentralized verification, QR Code authentication, anti-counterfeiting, digital certificate management.

1. Introduction

With internet being a necessary part of modern human life, unethical practices have also come to a rise. Our countermeasures to such unethical practices however haven't evolved as fast. Fake certificates, loans, online frauds, fake products etc have become rampant and it has become hard to deal with them as the vast and easy availability of internet has boosted such acts to a level that one can't easily differentiate to what is authentic and what is fake. This results in lack of trust and monetary loss for both parties while a unethical middle man gets benefits.

Certificates in educational institutions have been issued in the same way for decades now. Even after digitization of the records, the basic structure has remained same; this leads to producing fake and doctored certificates from individuals to take undue advantage of the degree.

This greatly hampers the hiring process for students where the companies have to employ background check services which verify the authenticity of the certificates almost entirely manually which aren't foolproof either. This results in delay in hiring process, which hampers both the companies and the students.

1.1 Problem Definition

The current centralized methods of certificate validation face challenges such as potential fraud, inefficiencies in verification processes, and a lack of transparency. Institutions struggle with the manual verification of certificates, and students face difficulties in securely maintaining and sharing their academic credentials. To address these issues, there is a need for a decentralized certificate validation system using the blockchain. This system aims to enhance security by leveraging blockchain's immutability and cryptographic features, streamline the validation process for institutions, and empower individuals to easily access and share their verified credentials. The decentralized nature of the proposed system ensures transparency, reduces the risk of fraud, and provides a more efficient and trustworthy method for validating academic certificates.

1.2 Existing System

If an organization is hiring an associate worker, they'll perform a background check. associate worker Background verification method could be a thorough screening of a candidate's work history within the past, education background and degrees, educational certificates, legal records, and most credit scores. The method sometimes takes between 3-10 days. This goes up just in case of intensive checks and for senior-level hires. Statistics show that almost all candidates aren't entirely truthful on their resumes and infrequently exaggerate their skills and talents. it's clear that education verification checks square measure essential build. employers make appropriate hiring choices. the corporate runs a background check on one's resume/CV, once all the interview rounds square measure qualified by the worker. an associate worker background check could be a review of a person's industrial, criminal, employment, and/or money records. Many employers conduct background checks on job candidates through third-party corporations that verify the candidate's background by confirming with the past executive department or university and visiting home address to verify the residence. Some employers conduct

checks when they need to be employed associate workers. large cash is spent by the corporate throughout this background verification method. So, there square measure tons of physical document checks while not knowing it's legit or authentic and it takes a large quantity of your time for verification. the most aim is to scale back of these large tasks and third-party involvement which can compromise the system to straightforward, direct, and secure interaction between an organization and also the candidate certificate.

1.3 Proposed System

Online Authentication of documents will reduce the investment of time during a background check. Since the world is getting digitized, the idea of online authentication of academic documents will help many students/institutes and also recruiters. In this model, while giving certificate to student, admin user will store certificate copy in Blockchain and obtained its digital signature and then generate QR code on that signature and affix that code on student certificate. This certificate can be scanned by other companies or institution to verify and extract details from Blockchain. If QR code exists in Blockchain then certificate validation will be successful.

Since the Certificates are in blockchain, Data immutability and Security are strictly maintained. Overall, developing a Decentralized application that is universally accessible for students/employers to view and verify academic certificates without any third-party involvement, which is very simple to use, also efficient will make a major impact in near future.

1.4 System Requirements

The software requirements are as follows:

- Visual Studio Community Version
- Nodejs (Version 12.3.1)
- Python IDEL (Python 3.7)
- LANGUAGES BACK-END: Python, Java Script, Solidity
- LANGUAGES FRONT-END: HTML, CSS, JS, Boot Strap
- FRAMEWORK: Flask or DJANGO

The hardware requirements are as follows:

- Operating System : Windows
- Processor : i5 and above
- Ram : 4gb and above
- Hard Disk : 50GB

2. Literature Survey

[1] **Khushal Y. Bheke, Aniket R. Misal, Nilkanth S. Pokharkar, Prof. Gunjal, "Digital Certificate Verification Using Blockchain Technology",2023.**

This presents a blockchain-driven solution for streamlined academic certificate verification. Accrediting bodies oversee universities, and certificates are encrypted using an AES cipher before being uploaded to the Ethereum blockchain. Students obtain encryption keys for accessing their certificates, and recruiters can use public hash values for instant verification. The system addresses the prevalent issue of fake certificates, aiming to enhance security, cut costs, and ensure the accuracy of digital certificates. The proposed model leverages smart contracts, SHA256 hash generation, and mining algorithms within a decentralized architecture. The study underscores the potential of blockchain technology in revolutionizing certificate management and verification processes for educational institutions and employers alike.

[2] **Jongbeen Han, Heemin Kim, Hyeonsang Eom, Yongseok Son, "A Decentralized Document Management System using Blockchain and Secret Sharing", 2021.**

Decentralized Document Management System (DDMS) aiming to enhance the security of digital documents. Leveraging blockchain technology, DDMS employs Shamir's secret sharing scheme to distribute access permissions among multiple users, increasing document security. The system encrypts documents using a symmetric key, splits the key via secret sharing, and manages the split keys on the blockchain. During document retrieval, smart contracts facilitate the reconstruction of the symmetric key. Experimental results on the Ethereum blockchain demonstrate that DDMS achieves higher security with a reasonable performance overhead compared to three other types of Document Management Systems (DMSs). The proposed approach addresses security issues such as forgery and data leakage, providing a decentralized solution for secure document management.

[3] **Priyanka Killedar, Pranav L M, Nachiketh S Bhat, Ravi Math, Shruti Shetty,"Blockchain Based Academic Certificate Authentication System",2021.**

The paper proposes a comprehensive solution to the pervasive issue of fake academic certificates through the integration of blockchain technology. In an

era dominated by digitalization, organizations often face challenges in verifying the authenticity of educational credentials. The proposed system suggests converting physical certificates into secure, immutable digital records stored on a blockchain, with Ethereum as the chosen platform. The architecture combines MongoDB Atlas, Truffle, Web3.js, SendGrid, and Infura to facilitate the creation, storage, and verification of digital certificates. The workflow involves administrators uploading academic details, generating unique Certificate IDs, and sending them to students. Employers can then verify certificates using the provided IDs. The system's potential benefits include reduced time and cost in the verification process, enhanced security, and the prevention of certificate fraud. The approach is positioned to revolutionize the verification of academic credentials by leveraging the transparency and security features inherent in blockchain technology.

[4] Roshani S. Bele, Jayant P. Mehare, "Automatic Digital Degree/ Documents Verification Using Ethereum Blockchain", 2021.

This paper addresses the prevalent issue of document forgery, specifically in the context of educational certificates in the Indian education system. With approximately 37 million students enrolling for graduation annually, the paper emphasizes the challenges associated with document verification during processes such as admission and job interviews. The authors propose a blockchain-based solution to enhance the security and efficiency of the document verification process. The system involves converting physical certificates into digital records stored on a blockchain, ensuring immutability and transparency. The proposed model allows users, including universities, students, and third-party verifiers, to participate in the certificate verification process. The authors highlight the advantages of blockchain, such as incorruptibility, encryption, and traceability, in minimizing document verification time and improving overall efficiency. The paper includes a detailed system design and process flow, illustrating how different users interact with the blockchain for document verification. The proposed solution aims to address security and efficiency issues in document verification, showcasing the potential of blockchain technology in the education sector.

[5] A.Gayathiri, J.Jayachitra, Dr.S.Matilda, "Certificate validation using Blockchain",2020.

It proposes a blockchain-based solution for enhancing the security and verification of academic certificates. In the current digital era, traditional certificates such as SSLC, HSC, and academic certificates are being digitalized, posing challenges for students to manage and institutions to verify. The project suggests converting paper certificates into digital certificates, utilizing a chaotic algorithm to generate hash codes for certificates, and storing them on a blockchain. The certificates can be validated using a mobile application, offering a more secure and efficient digital certificate validation process. The literature survey discusses existing systems using blockchain for certificate security, highlighting their strengths and limitations. The proposed system aims to leverage the unmodifiable property of blockchain for increased security, transparency, and rapid certificate validation, catering to the need for protecting against forgery in the education sector.

Table 1: Literature Survey

S.No	Title	Authors	Year	Merits	Demerits
1.	Digital Certificate Verification Using Blockchain Technology	Khushal Y. Bheke, Aniket R. Misal, Nilkanth S. Pokharkar, Prof. Gunjal	2023	Addresses fake academic certificates, employs secure SHA256 and IPFS, ensures transparency. Decentralized system cuts costs, prevents forgery, and provides accurate digital certificates.	Blockchain scalability, adoption challenges. Limited validation details. Integration hurdles with existing systems and regulations.
2.	A Decentralized Document Management System using Blockchain and Secret Sharing	Jongbeen Han, Heemin Kim, Hyeonsang Eom, Yongseok Son	2021	Decentralized access control via blockchain and Shamir's secret sharing enhances document security. Experimental results show improved security with reasonable performance.	Dependence on Ethereum blockchain raises scalability issues. Real-world applicability needs thorough validation beyond experimental results.
3.	Blockchain Based Academic Certificate Authentication System	Priyanka Killedar, Pranav L M, Nachiketh S Bhat, Ravi Math, Shruti Shetty	2021	Addresses fake certificates using blockchain, multi-signature authentication, and decentralized storage. Enhances trust, saves time, and reduces costs in certificate verification.	Assumes blockchain familiarity, potential user adoption challenges, lacks vulnerability discussion, effectiveness dependent on blockchain acceptance, scalability concerns unaddressed.
4.	Automatic Digital Degree/ Documents Verification Using	Roshani S. Bele, Jayant P. Mehare	2021	Innovative use of blockchain for secure certificate verification, reducing forgery risks, enhancing transparency.	Limited exploration of potential challenges or drawbacks. Real-world implementation issues and scalability concerns may not be

	Ethereum Blockchain			Decentralized system improves efficiency and data security in the education sector.	fully addressed in the proposed model.
5.	Certificate validation using Blockchain	A.Gayathiri, J.Jayachitra, Dr.S.Matilda	2020	Innovative use of blockchain for certificate security, efficient android app for certificate validation, integration of a chaotic algorithm for hash code generation.	Limited exploration of algorithm details, incomplete discussion of potential challenges, lack of real-world implementation insights.

3. Design Methodology

3.1 Blockchain

The concept of blockchain was proposed by Satoshi Nakamoto in 2008. Blockchain is an online ledger that provides decentralized and transparent data sharing. With distributed recordings, all transaction data (stored in nodes) are compressed and added to different blocks. Data of various types are distributed in distinct blocks, enabling verifications to be made without the use of intermediaries. All the nodes then form a blockchain with timestamps. The data stored in each block can be verified simultaneously and become inalterable once entered. The whole process is open to the public, transparent, and secure. The emergence of Ethereum Smart Contracts in 2013 boosted blockchain technology, which became blockchain 2.0. As presented in blockchain 1.0 was mainly adopted by Bitcoin to solve problems concerning cryptocurrencies and decentralized payments. Blockchain 2.0 focused on decentralizing the entire market and is employed to transform assets through smart contracts, thereby creating value through the emergence of alternatives to Bitcoin .

3.2 Ethereum

Ethereum is an open and decentralized platform featuring Turing completeness and supporting various derivative applications. Most smart contracts and decentralized autonomous organizations are created by using Ethereum. If the Bitcoin blockchains are considered a global payment network, Ethereum would be the global computing system. Furthermore, Ethereum is an opensource platform similar to Android (developed by Google). It provides an infrastructure that enables developers to create applications. The infrastructure is developed and maintained by both Ethereum and those developers.

The major characteristics of Ethereum are as follows:

- incorruptible: third-parties are not able to modify any data.
- secure: errors derived from personnel factors are avoided because the decentralized applications are maintained by entities rather than individuals.
- permanent: blockchain does not cease to operate even if an individual computer or server crashes.

1) Ethereum Virtual Machine (EVM)

The EVM is a programmable blockchain. Unlike Bitcoin, which provides a fixed set of commands, the EVM allows developers to run any programs in the manner they wish. Developers instruct the EVM to execute applications by using a high-level language called Solidity.

2) Solidity

Solidity is the programming language used for implementing smart contracts and is similar to JavaScript. After a Solidity-programmed smart contract is completed,

a compiler called solc is required to transform the Solidity code into contract bytecode, which is then interpreted by the EVM. Next, the compiled instructions are deployed in

an Ethereum blockchain. This completes the whole process.

3.3 Smart Contract

Smart contracts were first proposed by Nick Szabo in the early 1990s. He explained that a smart contract enabled computers to execute transaction clauses. As blockchain

has become popular, smart contracts have received increased attention. Smart contracts are the main feature of Ethereum, a blockchain platform founded in 2015. A

smart contract is “a digital contract that is written in source code and executed by computers, which integrates the tamper-proof mechanism of blockchain”.

Smart

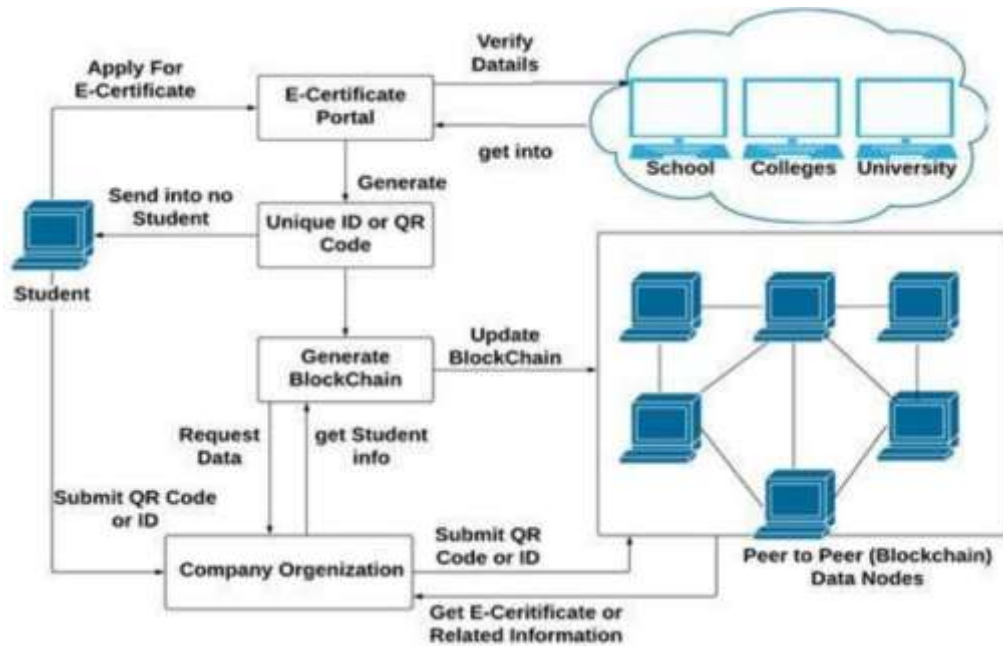
contracts can be created using the Ethereum blockchain. Developers are able, according to their needs, to specify any instruction in smart contracts; develop various types of applications, including those that interact with other contracts; store data; and transfer Ethers. Additionally, smart contracts that are deployed in blockchains are

copied to each node to prevent contract tampering. With related operations executed by computers and services provided by Ethereum, human error can be reduced to

avoid disputes regarding such contracts. Smart contracts are mostly used in voting system and cryptocurrency applications. The high-level programming languages used for writing smart contracts are mainly Solidity, Serpent, and LLL. Currently, most developers employ Solidity to write smart contracts and compile the instructions into bytecode for the EVM to execute. Certain costs are incurred when developers create smart contracts.

3.4 System Architecture

Figure 1: System Architecture of Decentralized Certificate Validation System using Blockchain



The Figure 1 describes a framework, where admin users upload certificates, receiving digital signatures and generating unique QR codes for verification. External entities scan QR codes, initiating validation against Blockchain records. If the QR code matches data stored in the Blockchain, certificate validation succeeds, affirming its authenticity. This approach enhances trust in certificates, as their integrity and origin are verifiable through decentralized Blockchain consensus, mitigating risks of forgery and unauthorized modifications. By using blockchain technology we can provide a more secure and efficient digital certificate validation.

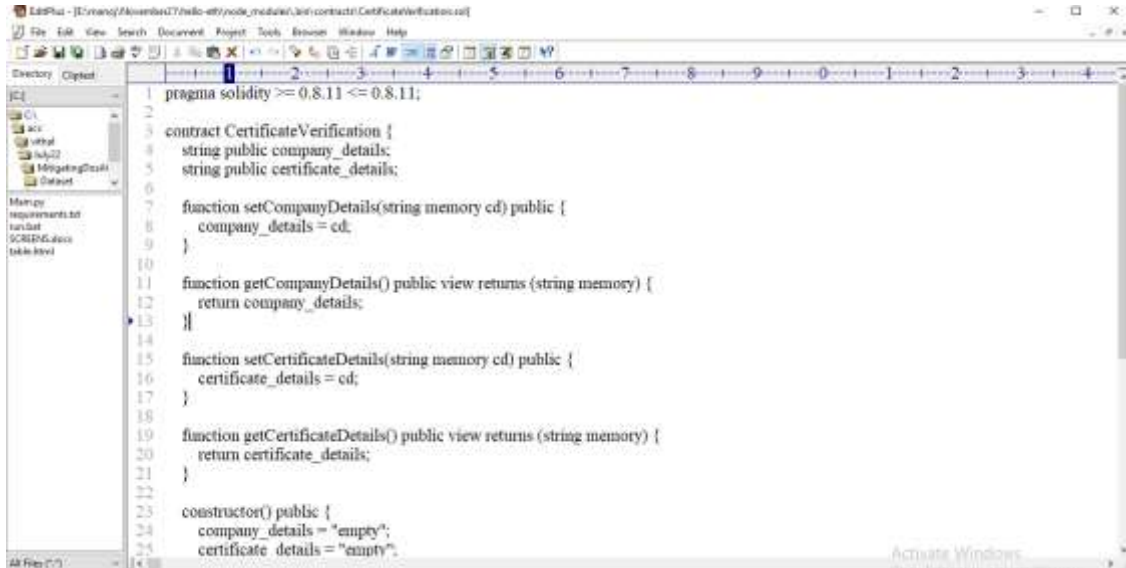
3.5 Modules

- 1) Admin: Admin is an education authority which login to system using username and password as 'admin' and 'admin'. After login admin will upload student details and certificate and this details will be uploaded to Blockchain and Blockchain associate each certificate with unique hash code called as digital signature. QR CODE will also be generated on Hashcode and affix on student certificate and this QR CODE can be scanned from mobile to get details from Blockchain and if QR CODE exists in Blockchain then certificate validation successful
- 2) Company: company user can signup and login to system and then scan and upload certificate and then application will generate digital signature and matched with those signature stored in Blockchain and if certificate is original then same signature will be generated and authentication will be successful.
- 3) Scanner Module: This is a standalone module which will maintain by education institution and companies and using this module they can scan QR CODE to get details from Blockchain.

4. Implementation and Results

4.1 Implementation

To store data in Blockchain we need to develop SOLIDITY contract which contains functions to STORE and authenticate certificate details. This solidity contract need to be deployed on Ethereum Blockchain and then it will return contract deployed ADDRESS and this address we can specify in PYTHON code to store and access certificate details.



```

1 pragma solidity >= 0.8.11 <= 0.8.11;
2
3 contract CertificateVerification {
4     string public company_details;
5     string public certificate_details;
6
7     function setCompanyDetails(string memory cd) public {
8         company_details = cd;
9     }
10
11    function getCompanyDetails() public view returns (string memory) {
12        return company_details;
13    }
14
15    function setCertificateDetails(string memory cd) public {
16        certificate_details = cd;
17    }
18
19    function getCertificateDetails() public view returns (string memory) {
20        return certificate_details;
21    }
22
23    constructor() public {
24        company_details = "empty";
25        certificate_details = "empty";
26    }
27 }

```

Figure 2: Solidity Code

In the Figure 2 , solidity code we have defined functions to store and access company and certificate details.

To deploy above contract in Ethereum we need to follow below steps:

Go inside 'hello-eth/node-modules/.bin' folder and then double click on 'runBlockchain.bat' file to start Ethereum tool and get below screen.



```

Select Command Prompt - truffle develop
(2) 0xc432c93aa581c68ed3f85fa8b212f3f41e1ec712
(3) 0x029fb6a3080361e87488fd7a61f1ece30b25d11d
(4) 0x2432dbdc222ffce4c5473423d1af5d56864a7f8
(5) 0x07179afb9cbe0904764853551a70881ab0f70ef8
(6) 0x726facb8dea3534b86e72d2df7e863cf497ed9b3
(7) 0x55f4b977e6c8a1ccccbecb180abdb2a67f7ba2d3
(8) 0x5f9eb3646fdc53c384783f38f46886431003e425
(9) 0xb94279d4329857278b8b8c8ec22ac90e97ac89

Private Keys:
(0) b0f17ca0eb13a6788828dd1d59f520caef17029835d405f9e21d350b60fcd5e
(1) 1aefa2209d068ef6c98b15e8a590eb49fd973d09e4079d439e8384b11aa6381
(2) 3721b88873a2d7e1907a4006f720fd5852a639fe6b69cb1d5d52f7284daf81f5
(3) bba83a797a8b0dba41f209b3d813e3a1346b4d015edb55a7c56e36b085aa7966f
(4) 77fe4d767986f96c3ec178db1dba5da803d91b3f27f550e4e0c11ee2ca58cc2c
(5) 5703fbbd3d8812ef787fb7c1f87bfb3d660d053639ca4748b422c7eb5f490d2
(6) b337a06d579c2a284d625ac11eae730a81854cb5febcbac382d90a2d8202543
(7) 5cf4d9e90b5f38c4a69f340665f84a713e9b3f2f491ff0c10b7abe18c4221afe
(8) 834bb791489ad5bf545225108db6a50e237456418bc3ab957999245a6d3ed527
(9) 3b3852138739d1c84d1ee9349e4bf3fdb9f61f5059f20d8eeba0da31e1de4c05

Mnemonic: repeat kitten art call plastic talent gather cannon cabbage stove find convince
Important : This mnemonic was created for you by Truffle. It is not secure.
Ensure you do not use it on production blockchains, or else you risk losing funds.

truffle(develop)> truffle migrate

Compiling your contracts...

```

Figure 3: Starting Ethereum Tool

In Figure 3 , we can see Ethereum generate some default ADDRESS and private keys and in above screen type command as 'truffle migrate' and press enter key to deploy contract and will get below output.

```

Select Command Prompt - tralix develop
> Saving artifacts
-----
> Total cost:      0.000497788 ETH

2_deploy_contracts.js
-----
Deploying 'CertificateVerification'
-----
> transaction hash:  0xdf10a8353217868f495a810193666a396ea88c04c774a322b94ba1ab6f5a10f5
> Blocks: 0
> contract address: 0x1004fb45C1cdC8C3F32cbaA60464c8107D4D4058
-----
> block number:      3
> block timestamp:   1659073276
> account:           0xc7B56c1B125271E1dE0ffA10a84a83cC620313f
> balance:           99.990434508
> gas used:          491339 (0x77f4b)
> gas price:         2 gwei
> value sent:        0 ETH
> total cost:        0.000982678 ETH

> Saving migration to chain.
> Saving artifacts
-----
> Total cost:        0.000982678 ETH

```

Figure 4: Deploying Contract

In Figure 4, in white colour text we can see 'Certificate Verification' contract deployed and we got contract address also and this address we will specify in Python code to access that contract.

```

C:\Windows\system32\cmd.exe
C:\Users\November21\CertificateVerification>python Main.py
 * Serving Flask app "Main" (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployment.
   Use a production WSGI server instead.
 * Debug mode: off
 * Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)

```

Figure 5: Flask server started

In Figure 5, python FLASK server started and now open browser and enter URL as <http://127.0.0.1:5000/index>

4.2 Results

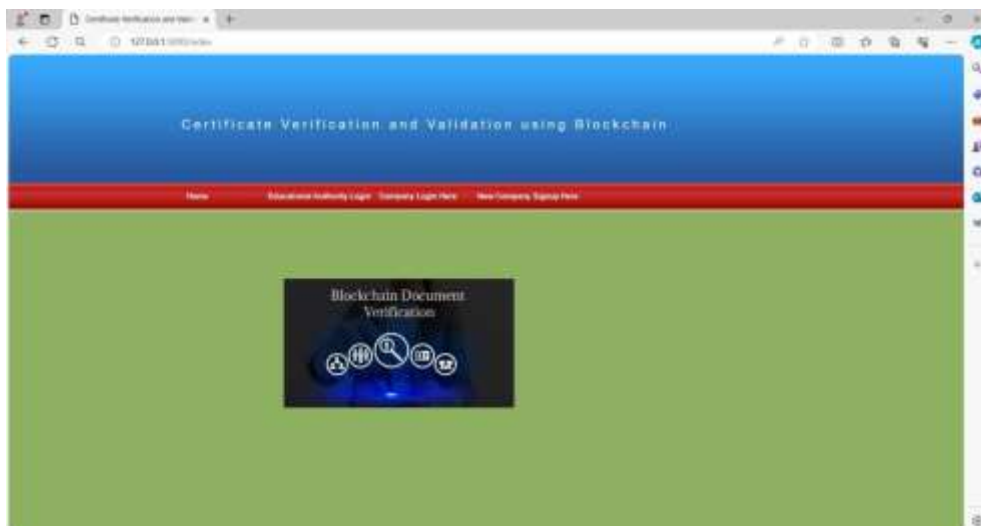


Figure 6: Home page of certificate validation system using Blockchain

In Figure 6 student details are added and we can see digital signature generated and stored in Blockchain for uploaded certificates and now admin can click on 'Click Here to Download QR Code image' button to download QR Code.

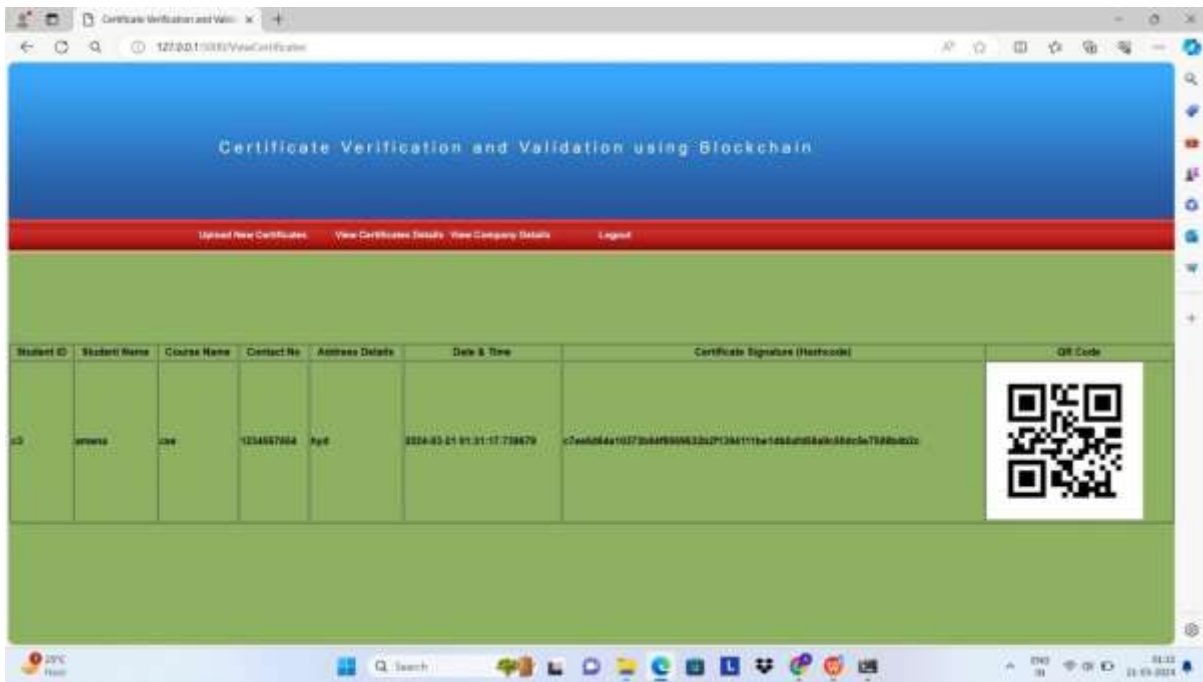


Figure 7: Certificate Details

In Figure 7 we can see different certificates of same or new student stored in Blockchain and we can see date and time of upload with digital signature and QR CODE image.

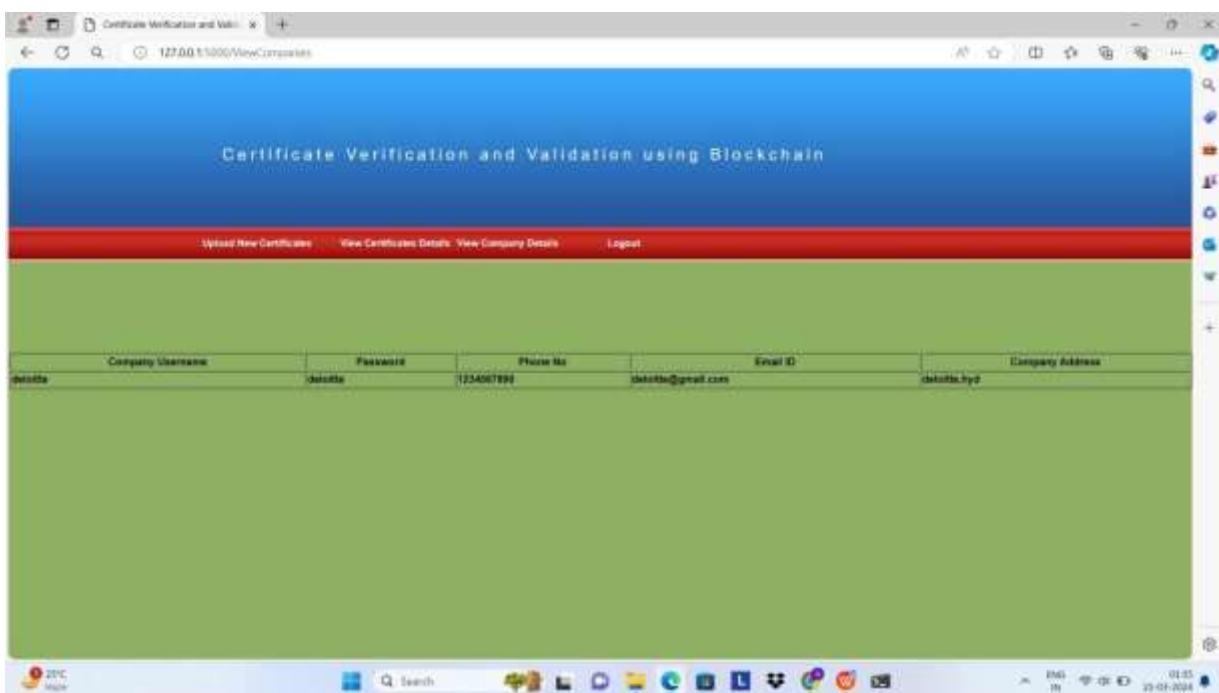


Figure 8: Company Details

In Figure 8 admin can view list of registered companies.



Figure 9: Company Signup

In Figure 9 company is entering signup details and press Submit button to store details in Blockchain.



Figure 10: Company Login page

In Figure 10 company is login.

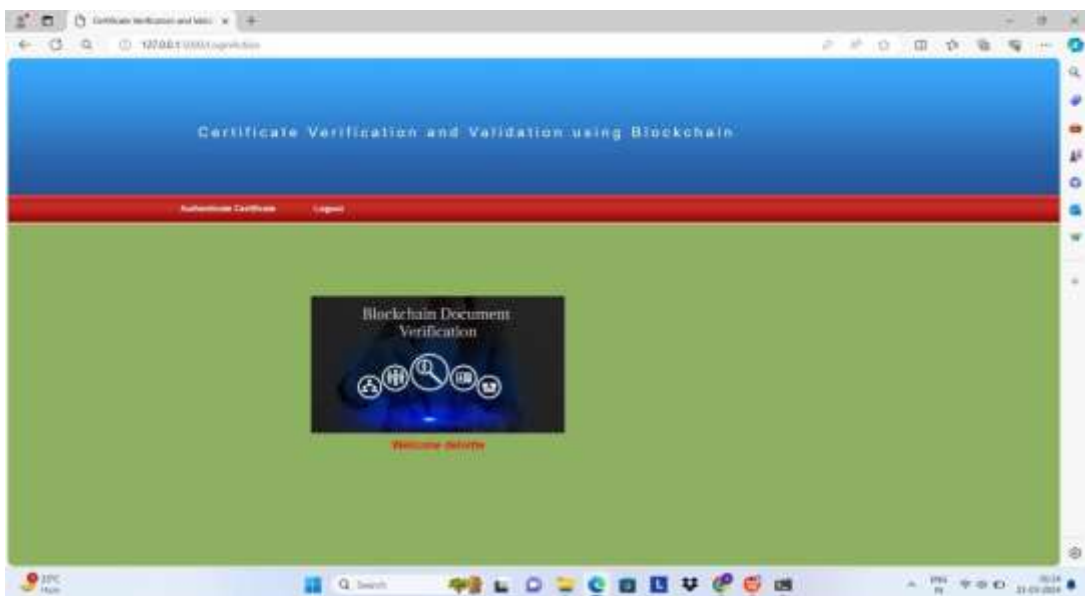


Figure 11: Company Login

In Figure 11 company can click on 'Authenticate Certificate' to upload certificate copy received from student and perform verification.



Figure 12: Authenticate Certificate Screen

In Figure 12 company can upload certificate and get below details if authenticated.

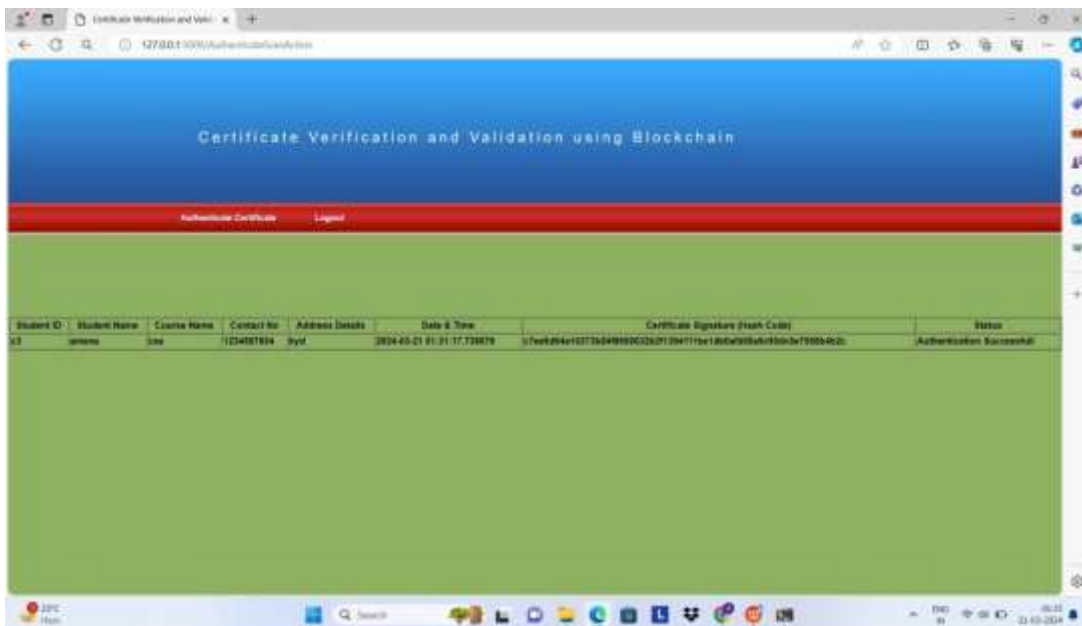


Figure 13: Authentication Successful

In Figure 13 company can view all details of uploaded certificated and in last column we can see authentication successful and similarly they can upload and verify any certificate.

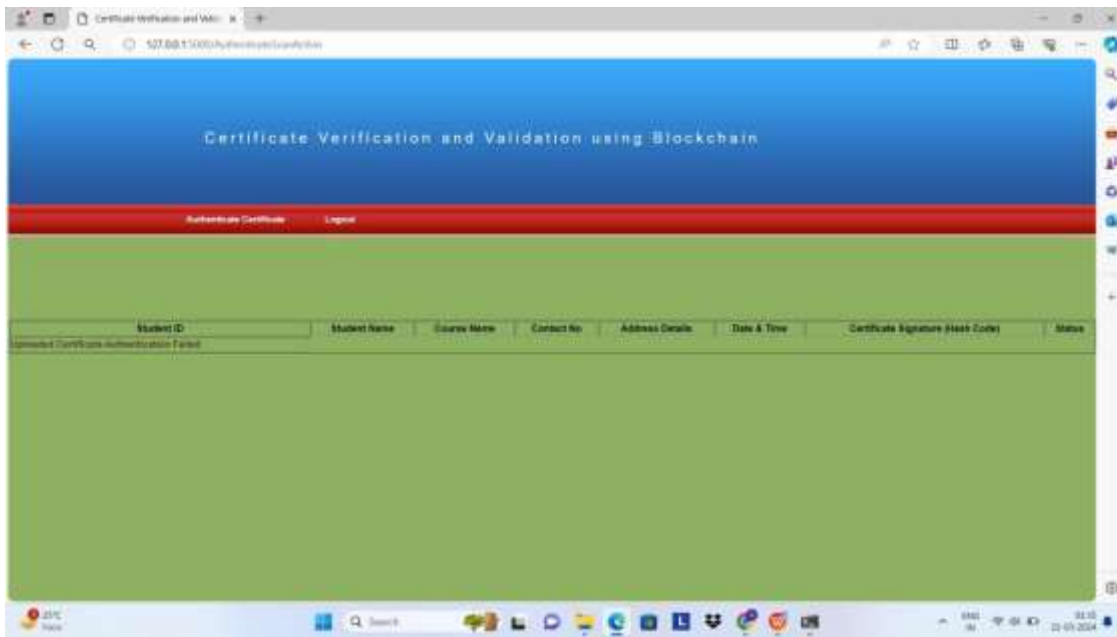


Figure 14: Authentication Failed

In Figure 14 we can see Authentication failed for uploaded certificate.

Now company or educational institution can validate certificate by scanning QR code and to do that, just double click on 'RunWebCam.bat' file

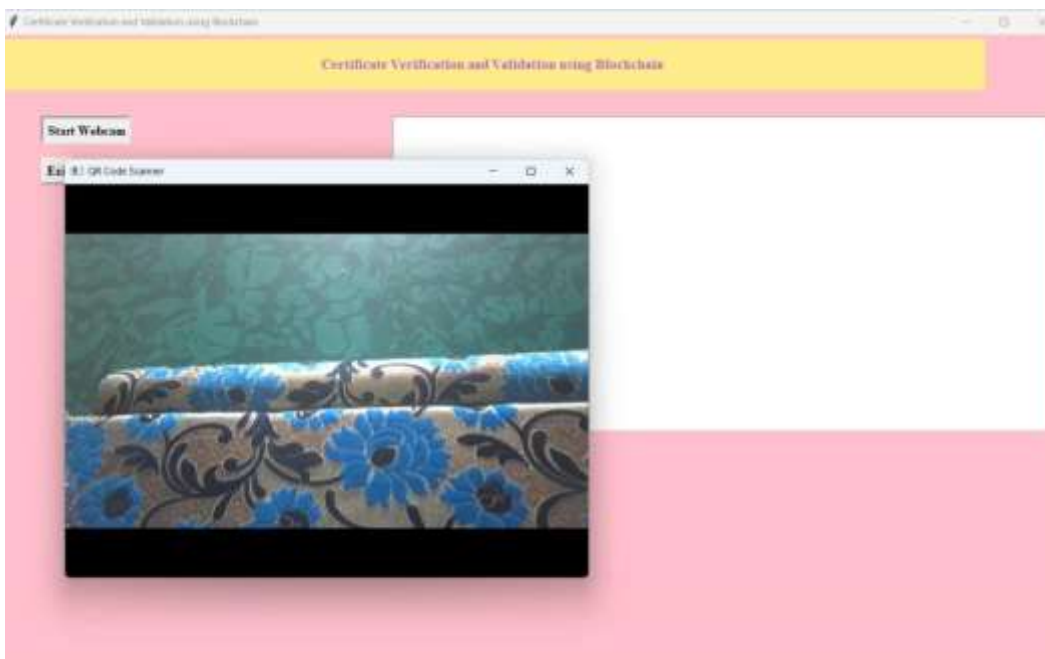


Figure 15: Starting Webcam

In Figure 15 webcam , they need to scan QR CODE from mobile .



Figure 16: Certificate Verification Successful

In Figure 16 once we show QR code then all details for that QR code certificate will be retrieve from Blockchain and display in above TEXT area.



Figure 17: Certificate Verification Failed

Similarly if we scan wrong QR CODE then will get message as Certificate verification failed as QR code does not exists as shown in Figure 17.

5. Conclusion

Data security is one of the major features of blockchain technology. Blockchain is a large and open-access online ledger in which each node saves and verifies the same data. Using the proposed blockchain-based system reduces the likelihood of certificate forgery. The process of certificate application and automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In conclusion, the system assures information accuracy and security

6. Future Scope

The proposed solution can highly benefit students and employers to make verification of documents faster and easier than the existing solution. It'll also reduce manipulation and other unethical practices with educational certificates.

This solution will not only benefit university certificates, but the same framework can be extended to other important documents, exclusive products, loans, etc.

While blockchain technology is still pretty new, significant work is being carried out to make blockchains even more closer to reality. In present day it is not too cost effective to add data to blockchain, but with gradual advancement in technology and computing power, blockchain is slowly but steadily making way into our daily lives.

References

- [1] Khushal Y. Bheke, Aniket R. Misal, Nilkanth S. Pokharkar, Prof. Gunjal, "Digital Certificate Verification Using Blockchain Technology", International Journal of Research Publication and Reviews, Vol 4, no 5, pp 3722-3726 May 2023.
- [2] Jongbeen Han, Heemin Kim, Hyeonsang Eom, Yongseok Son, "A Decentralized Document Management System using Blockchain and Secret Sharing", Proceedings of the ACM Symposium on Applied Computing, pp.305-308 March 2021.
- [3] Priyanka Killedar, Pranav L M, Nachiketh S Bhat, Ravi Math, Shruti Shetty, "Blockchain Based Academic Certificate Authentication System", IJCRT, Volume 9, ISSN: 2320-2882, Issue 7 July 2021.
- [4] Roshani S. Bele, Jayant P. Mehare, "Automatic Digital Degree/ Documents Verification Using Ethereum Blockchain", International Journal for Innovative Research in Multidisciplinary Field ISSN: 2455-0620 Volume - 7, Issue - 5, May 2021.
- [5] A. Gayathiri, J. Jayachitra, Dr. S. Matilda, "Certificate validation using Blockchain", IEEE 7th International Conference on Smart Structures and Systems ICSSS 2020.
- [6] Rui Xie, Yuhui Wang, Mingzhou Tan, Wei Zhu, Zhongjie Yang, Jiayi Wu, and Gwanggil Jeon, "Ethereum-Blockchain-Based Technology of Decentralized Smart Contract Certificate System", IEEE Internet of Things Magazine 3(2):44-50 June 2020.
- [7] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate", IEEE International Conference on Applied System Invention (ICASI), 17 April 2018.
- [8] D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, "Certificate Transparency Using Blockchain", IEEE International Conference on Data Mining Workshops (ICDMW), 1 November 2018.
- [9] Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain", Journal of Physics Conference Series 1069(1):012125, August 2018.
- [10] Xiuping Lin, "Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the Ethereum Blockchain", Department of Information Engineering, National Taiwan University, Taiwan, R.O.C., 2017.
- [11] Yong Shi, "Secure storage service of electronic ballot system based on block chain algorithm", Department of Computer Science, Tsing Hua University, Taiwan, R.O.C., 2017.
- [12] Zhenzhi Qiu, "Digital certificate for a painting based on blockchain technology", Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C., 2017.
- [13] Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.