Enhancing Trust and Integrity in Educational Certification Systems with Blockchain Credentials

A Project Report Submitted in the
Partial Fulfillment of the Requirements
for the Award of the Degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Submitted by

Rakesh Modi	**20881A05N0**
Nikhil Badam	**20881A05J5**
Sayyed Shoheb	**20881A05P4**

SUPERVISOR
Ms. Rayeesa Tasneem
Assistant Professor

Department of Computer Science and Engineering

VARDHAMAN COLLEGE OF ENGINEERING
(AUTONOMOUS)
Affiliated to JNTUH, Approved by AICTE, Accredited by NAAC with A++ Grade, ISO 9001:2015 Certified
Kacharam, Shamshabad, Hyderabad – 501218, Telangana, India

April, 2024

VARDHAMAN COLLEGE OF ENGINEERING
(AUTONOMOUS)
Affiliated to JNTUH, Approved by AICTE, Accredited by NAAC with A++ Grade, ISO 9001:2015 Certified
Kacharam, Shamshabad, Hyderabad – 501218, Telangana, India

Department of Computer Science and Engineering

CERTIFICATE

This is to certify that the project titled **Enhancing Trust and Integrity in Educational Certification Systems with Blockchain Credentials** is carried out by

Rakesh Modi	**20881A05N0**
Nikhil Badam	**20881A05J5**
Sayyed Shoheb	**20881A05P4**

in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering** during the year 2022-23.

Signature of the Supervisor
Ms. Rayeesa Tasneem
Assistant Professor

Signature of the HOD
Dr. Ramesh Karnati
Associate professor and Head, CSE

Project Viva-Voce held on _____

Examiner

Acknowledgement

The satisfaction that accompanies the successful completion of the task would be put incomplete without the mention of the people who made it possible, whose constant guidance and encouragement crown all the efforts with success.

We wish to express our deep sense of gratitude to **Ms. Rayeesa Tasneem**, Assistant Professor and Project Supervisor, Department of Computer Science and Engineering, Vardhaman College of Engineering, for his able guidance and useful suggestions, which helped us in completing the project in time.

We are particularly thankful to **Dr. Ramesh Karnati**, the Head of the Department, Department of Computer Science and Engineering, his guidance, intense support and encouragement, which helped us to mould our project into a successful one.

We show gratitude to our honorable Principal **Dr. J.V.R. Ravindra**, for providing all facilities and support.

We avail this opportunity to express our deep sense of gratitude and heartful thanks to **Dr. Teegala Vijender Reddy**, Chairman and **Sri Teegala Upender Reddy**, Secretary of VCE, for providing a congenial atmosphere to complete this project successfully.

We also thank all the staff members of Computer Science and Engineering department for their valuable support and generous advice. Finally thanks to all our friends and family members for their continuous support and enthusiastic help.

Rakesh Modi

Nikhil Badam

Sayyed Shoheb

Abstract

Blockchain technology has emerged as a powerful tool for securing and validating digital transactions across diverse industries, including education. In response to the rising concerns surrounding fraudulent certificates and their detrimental impact on trust and credibility, this paper introduces a comprehensive blockchain-based system specifically tailored for the issuance and verification of educational certificates.By harnessing the capabilities of Ethereum for smart contract functionality, IPFS for decentralized storage, Flask for web application development, and Truffle for smart contract deployment and testing, our system addresses the pressing need for a secure and reliable certification process. While fraudulent certificates pose a significant threat to the integrity of educational qualifications, our system offers a solution that mitigates this risk through robust authentication mechanisms and transparent verification processes.Unlike traditional paper-based or centralized digital certificates, our blockchain-based system ensures the immutability and tamper-proof nature of educational credentials. By streamlining the entire certification lifecycle—from university registration to certificate sharing among students, employers, and educational institutions—we provide stakeholders with a trusted platform to validate the authenticity of certificates.Moreover, our focus on educational certificates is driven by the increasing prevalence of fraudulent practices in the hiring process. With the proliferation of false credentials used by job applicants to secure employment, companies face significant challenges in verifying the qualifications of potential hires. By prioritizing the verification of educational certificates, our system aims to restore trust in the recruitment process and safeguard the integrity of professional qualifications.

Keywords:Decentralized process,Document verification,Blockchain,Ethereum,Smart contracts,Hashing,IPFS.

Table of Contents

List of Figures

Abbreviations

Abbreviation	Description
IPFS	InterPlanetary File System
UML	Unified Modeling Language
DFD	Data Flow Diagram

CHAPTER 1

Introduction

1.1 Overview

The genesis of Blockchain technology can be traced back to the pioneering work of research scientists Stuart Haber and W. Scott Stornetta. However, its widespread acknowledgment surged with the advent of Bitcoin by the pseudonymous Satoshi Nakamoto in 2009. In the educational realm, Blockchain technology has found multifarious applications, spanning from the issuance and validation of e-transcripts to cost-effective storage of voluminous files. It has also revolutionized learning platforms by automating processes and providing mechanisms for publishing and safeguarding copyrights, alongside facilitating transactions through cryptocurrencies.

Traditional methodologies of dispensing paper-based degrees and certificates, followed by laborious manual verification procedures, are fraught with inefficiencies[1]. This antiquated system necessitates copious paperwork, numerous emails, and extensive phone calls, resulting in a protracted and cumbersome verification process. Moreover, this conventional approach is plagued by issues such as certificate misplacement or damage, thereby mandating re-issuance and exacerbating the quandary. Furthermore, the pervasiveness of document forgery undermines the integrity of credentials, consequently enabling the employment of unqualified individuals, which can incur substantial financial losses for companies, averaging around $15,000 USD$.

Studies have indicated alarmingly high rates of falsified degrees, with over 30 percent of claimed credentials found to be fabricated. Incidents such as the legal action against a court clerk in 2009 for fabricating documents to secure employment, or the resignation of MIT's Dean of Admissions Marilee Jones after the revelation of her misrepresented qualifications from a New York university for nearly three decades, underscore the imperative need for digitally

verifiable credentials. Research conducted by Ezell and Bear accentuates the lucrative nature of the billion-dollar industry fueling these deceptive practices.

The objective of this paper is to proffer a solution to the challenges entrenched within traditional paper-based educational certificates, leveraging blockchain technology, specifically on the Ethereum platform. The aim is to augment efficiency in the verification process, diminish the likelihood of document loss or damage, and mitigate forgery through the creation of secure and readily verifiable digital certificates. By harnessing Ethereum and smart contracts, this proposed solution endeavors to transform certificates into impregnable digital formats, ensuring streamlined verification processes and mitigating the inherent risks associated with paper-based documents.[2]

In the educational sector, traditional methods of issuing paper certificates have long been plagued by inefficiencies. These include time-consuming manual verification processes and the vulnerability of documents to loss or damage. Such challenges not only hinder the verification of credentials but also create opportunities for fraudulent activities, ultimately undermining the integrity of the education system.

However, the advent of blockchain technology offers a promising solution to these longstanding issues. By leveraging blockchain, educational institutions can transition from paper-based certificates to secure digital formats. This not only streamlines the verification process but also reduces the risk of document manipulation or forgery. Furthermore, the decentralized nature of blockchain ensures that certificates remain tamper-proof and easily accessible, thereby enhancing the overall trust and credibility of educational credentials.

By embracing blockchain technology, educational institutions can usher in a new era of efficiency and security in certificate issuance and verification. This not only benefits students and employers but also strengthens the foundation of the education system as a whole. With blockchain, the era of paper certificates may soon become a relic of the past, replaced by a more reliable and transparent system that meets the demands of the digital age.

1.2 Objectives

The objective of a project or initiative is a specific, measurable, achievable, relevant, and time-bound goal that guides its planning, execution, and evaluation. Objectives provide clarity on what needs to be accomplished and serve as a roadmap for success. They help stakeholders understand the purpose and scope of the project and ensure that efforts are aligned towards achieving tangible outcomes. Objectives should be realistic and achievable within the constraints of resources, time, and other factors. Additionally, they should be periodically reviewed and updated as needed to reflect changes in circumstances or priorities. Overall, clear and well-defined objectives are essential for driving progress, measuring success, and ultimately achieving the desired impact of the project or initiative.[3]

1.2.1 Transition to Digital Certificates

This objective focuses on leveraging blockchain technology to transition from traditional paper certificates to secure digital formats. By digitizing certificates, educational institutions can streamline the issuance process, eliminating the need for physical documents. Digital certificates can be easily accessed and verified online, saving time and resources for both students and institutions. Additionally, digital certificates offer greater flexibility, allowing students to conveniently share their credentials with employers or other institutions as needed. Overall, transitioning to digital certificates enhances accessibility and efficiency in the certification process.[4]

1.2.2 Enhance Verification Efficiency

The objective here is to develop a blockchain-based system that significantly improves the efficiency of certificate verification. Blockchain technology provides features such as immutability and transparency, which enable quick and reliable verification of certificates. By storing certificate data on the blockchain, institutions can eliminate the need for manual verification processes, reducing administrative burdens and processing times. This enhances

the overall efficiency of the verification process, enabling institutions to validate credentials more quickly and accurately.[5]

1.2.3 Ensure Data Integrity and Security

This objective aims to utilize blockchain's inherent features, such as decentralization and cryptographic hashing, to ensure the integrity and security of certificate data. Blockchain technology provides a tamper-proof and transparent ledger, where certificate records are securely stored and cannot be altered without consensus from the network. This ensures that certificate data remains immutable and trustworthy, mitigating the risks associated with document tampering or forgery. By leveraging blockchain for data storage and verification, institutions can enhance the overall security and reliability of their certification processes.[6]

1.2.4 Facilitate Cross-Institutional Collaboration

The objective here is to create a platform that enables seamless collaboration and data sharing among educational institutions, employers, and other relevant parties. By leveraging blockchain's decentralized nature, the system aims to facilitate trusted interactions and information exchange across institutions. This promotes transparency and cooperation within the education ecosystem, allowing institutions to securely share verified credential data with employers or other institutions as needed. Cross-institutional collaboration enhances the overall efficiency and effectiveness of the certification process, fostering a more interconnected and reliable education system.[7]

1.2.5 Empower Students with Ownership and Control

This objective focuses on empowering students by granting them ownership and control over their digital certificates. Through self-sovereign identity principles and blockchain-based credential wallets, students can securely manage and share their certificates as needed. This reduces dependency on centralized authorities and enhances privacy, as students have full control over who can access their credential data. Empowering students with ownership and

control promotes trust and accountability in the certification process, allowing individuals to confidently manage their credentials throughout their academic and professional journeys.[8]

1.3 Scope of Project

The scope of our project encompasses the development and implementation of a blockchain-based system for the issuance and verification of educational certificates. This entails leveraging Ethereum blockchain technology to create a decentralized platform that offers immutability, decentralization, and tamper-proof documentation. Within this scope, the project aims to address two primary shortcomings observed in the current methods of certificate issuance and verification within the education sector: the prevalence of fraudulent certificates and the inefficiency of traditional paper-based verification processes.[9]

Key components of the project scope include the design and development of smart contracts using Solidity, a language specifically designed for Ethereum. These smart contracts will facilitate the creation and storage of digital certificates on the blockchain, ensuring their authenticity and integrity. Additionally, the project will utilize IPFS (InterPlanetary File System) to store the actual certificates, overcoming the size limitations of public blockchains like Ethereum.

The scope also encompasses the creation of a user-friendly interface for various stakeholders, including issuers (universities/colleges), document/degree receivers (students), and document verifiers (employers). This interface will enable issuers to create digital certificates for students, assign unique identifiers such as Certificate IDs and Transaction hash values, and securely transmit them through the blockchain network. Students, on the other hand, will be able to request, receive, and share their certificates with prospective employers or other entities, thus streamlining the certification process.[10]

Furthermore, the project scope includes mechanisms for secure verification of certificates by employers or other verifiers. Employers will be able to authenticate certificates using either the Certificate ID or Transaction hash value, ensuring the authenticity and integrity of the documents. This streamlined verification process significantly reduces the time and resources required for

manual verification, thereby enhancing efficiency and trust in the certification process.

Overall our project encompasses the design, development, and implementation of a comprehensive blockchain-based system for certificate issuance and verification in the education sector. By leveraging blockchain technology, the project aims to enhance security, efficiency, and trustworthiness in the management of educational certificates, ultimately revolutionizing the certification process for stakeholders involved.[11]

CHAPTER 2

Literature Survey

2.1 Educational imposters and fake degrees

In further examining the phenomenon of misrepresented educational credentials, it becomes evident that the socio-demographic characteristics of individuals engaging in such behavior align closely with Merton's theory of innovative deviance. This theory suggests that individuals who falsely assert credentials often do so as a means of achieving societal goals or expectations through unconventional means. Rather than being driven by a lack of status or recognition, these individuals may seek to circumvent traditional pathways to success by presenting themselves as more qualified than they actually are. This underscores the complex interplay of societal norms, personal motivations, and institutional pressures that contribute to the prevalence of fraudulent degrees.[12]

Moreover, the prevalence of fraudulent degrees poses significant challenges to both individuals and institutions within the education sector. For individuals, the consequences of being exposed as imposters can be severe, leading to reputational damage, legal repercussions, and professional setbacks. Similarly, institutions face reputational risks and potential legal liabilities if their graduates are found to have misrepresented their credentials. This highlights the need for robust verification mechanisms and proactive measures to combat fraud and maintain the integrity of educational credentials.

In response to these challenges, there is a growing recognition of the importance of implementing technological solutions, such as blockchain, to enhance the verification and authentication of educational credentials. By leveraging blockchain's decentralized and immutable ledger system, institutions can establish a secure and transparent platform for storing and verifying academic records. This not only reduces the risk of fraud but also streamlines the

verification process, thereby enhancing trust and reliability in the credentialing system. As such, the adoption of blockchain technology represents a promising avenue for addressing the pervasive issue of fraudulent degrees and ensuring the integrity of educational credentials in the digital age.[13]

Upon deeper examination, it becomes apparent that the misrepresentation of educational credentials is often driven by complex socio-demographic factors, as outlined in Merton's theory of innovative deviance. This theory posits that individuals may resort to falsely asserting credentials as a means of navigating societal expectations and achieving success through unconventional avenues. Rather than solely seeking recognition or status, these individuals may exploit alternative routes to advancement by exaggerating their qualifications. This highlights the nuanced interplay between societal norms, individual aspirations, and institutional pressures, underscoring the multifaceted nature of fraudulent degrees.[14]

Furthermore, the prevalence of fraudulent degrees poses multifaceted challenges to both individuals and educational institutions. Individuals who engage in credential misrepresentation risk facing severe consequences, including damaged reputations, legal consequences, and professional setbacks, upon exposure. Similarly, educational institutions confront reputational risks and potential legal liabilities if their graduates are found to have misrepresented their credentials. In light of these challenges, there is a pressing need for robust verification mechanisms and proactive measures to combat fraud and uphold the integrity of educational credentials.[15]

In response to these challenges, there is a growing acknowledgment of the significance of technological solutions, particularly blockchain technology, in enhancing the verification and authentication of educational credentials. By harnessing blockchain's decentralized and immutable ledger system, institutions can establish a secure and transparent platform for storing and verifying academic records. This not only mitigates the risk of fraud but also streamlines the verification process, bolstering trust and reliability in the credentialing system. Thus, the adoption of blockchain technology holds immense promise in addressing the pervasive issue of fraudulent degrees and safeguarding the

integrity of educational credentials in the digital age.[16]

2.2 CredenceLedger: A Private Blockchain for Valid Academic Credentials

Blockchain technology has indeed garnered widespread attention due to its transformative potential across various sectors. Initially associated with cryptocurrencies like Bitcoin and Ethereum, blockchain's utility extends far beyond digital currencies. Its decentralized and immutable nature makes it a suitable solution for addressing challenges in finance, e-commerce, IoT, healthcare, and governance. The core characteristics of blockchain, including decentralization, immutability, security, and transparency, make it an attractive option for innovating various industries, including education.[17]

In the realm of education, blockchain technology offers immense promise for revolutionizing the verification of academic credentials. 'CredenceLedger,' a proposed blockchain solution, aims to capitalize on these inherent features. By securely storing concise data proofs of digital academic credentials within a permissioned blockchain ledger, CredenceLedger ensures that only authorized parties can access and validate these credentials. This approach not only safeguards sensitive information but also maintains transparency and trust within the credential verification process.[18]

Moreover, CredenceLedger introduces a decentralized verification system for academic credentials. This system allows educational stakeholders and third-party organizations to readily verify credentials without the need for intermediaries. By eliminating intermediaries, CredenceLedger streamlines the verification process, reducing the risk of fraud and enhancing the overall security and integrity of academic credentials. This decentralized approach enhances efficiency and trust, establishing a new standard for credential verification in the digital age.

In essence, CredenceLedger represents a paradigm shift in credential verification, leveraging blockchain technology to provide a tamper-proof and transparent platform. By offering a secure and reliable solution for storing and

verifying academic credentials, CredenceLedger fosters trust and confidence among educational stakeholders. As blockchain continues to evolve and gain traction, solutions like CredenceLedger are poised to reshape the educational landscape, ushering in a new era of trust and transparency in credential verification.[19]

2.3 Using blockchain as a tool for tracking and verification of official degrees: business model

The rising number of universities, tertiary education students, and graduates worldwide has created a significant demand for easily verifiable degree certificates. This demand presents a lucrative opportunity for businesses to leverage blockchain technology, particularly through the implementation of blockcerts software, to address the need for streamlined verification processes. By introducing two financial models, this paper aims to strike a balance in pricing between the primary stakeholders in the certification process: graduates and employers. Graduates seek cost-effective and easily verifiable proof of certification, while employers require quick and reliable verification of degrees during the recruitment process.[20]

The first financial model focuses on providing affordable certification services to graduates, aiming to incentivize widespread adoption of blockchain-based certificate verification. By offering competitive pricing tailored to the economic realities of different geographic markets, this model ensures accessibility for graduates seeking to authenticate their academic credentials. Simultaneously, the model incorporates mechanisms for revenue generation through volume-based pricing structures, thereby ensuring the sustainability and scalability of the certification service.[21]

In contrast, the second financial model targets employers by offering premium verification services tailored to their specific needs. This model emphasizes the value proposition of blockchain-based certificate verification in enhancing the efficiency and reliability of the recruitment process. Employers are willing to pay a premium for access to verified and tamper-proof degree

certificates, as this significantly reduces the time and resources expended on manual verification procedures. Additionally, the model may include value-added services such as background checks and credential verification, further enhancing its appeal to employers.[22]

Both financial models are designed to cater to various scenarios and geographic markets within the European Union, recognizing the diverse needs and preferences of stakeholders across different regions. By striking a balance between affordability for graduates and value for employers, these models aim to foster the widespread adoption of blockchain technology for certificate verification while creating viable business opportunities within the burgeoning certification market.

The adoption of blockchain technology, particularly through the implementation of an electronic authentication system, marks a significant milestone for Al-Zaytoonah University of Jordan. By embracing blockchain's decentralized and immutable nature, the university can establish a secure and integrated repository for its official documents. This transition represents a transformative shift in document management practices, offering enhanced security and integrity for a wide range of documents issued by university departments.[23]

Moreover, the implementation of blockchain-based solutions addresses long-standing concerns surrounding document security and information integrity. By leveraging blockchain's cryptographic protocols and consensus mechanisms, Al-Zaytoonah University can effectively mitigate the risk of data tampering, unauthorized access, or forgery. This not only ensures the authenticity of official documents but also instills trust and confidence among stakeholders in the university's document management practices.

Furthermore, the adoption of SmartCertBlockChain presents opportunities for innovation and collaboration within the university ecosystem. By embracing emerging technologies, Al-Zaytoonah University can foster a culture of digital transformation and excellence, positioning itself as a leader in educational innovation. This shift towards blockchain-based solutions not only enhances operational efficiency but also opens doors to new possibilities for academic research, collaboration, and knowledge dissemination.

Additionally, the integration of blockchain technology offers tangible benefits for academic research and collaboration. With a secure and transparent platform for document management and verification, researchers and educators can streamline processes related to data sharing, intellectual property rights, and scholarly communication. This facilitates greater collaboration and innovation within the academic community, ultimately contributing to the advancement of education and scholarship on a global scale.[24]

In summary, the adoption of SmartCertBlockChain represents more than just a technological upgrade for Al-Zaytoonah University. It signifies a commitment to excellence, innovation, and transparency in document management practices. By embracing blockchain technology, the university is not only enhancing the security and integrity of its official documents but also fostering a culture of digital transformation and collaboration within the academic community.

2.4 Blockchain and smart contract for digital certificate

The integration of blockchain technology into the certification process presents a significant advancement in addressing the vulnerabilities inherent in traditional paper-based certificates. With the increasing digitization of academic credentials, ensuring the integrity and authenticity of certificates has become paramount. By leveraging blockchain's immutable ledger, the proposed digital certificate system provides a robust and tamper-proof repository for storing academic credentials securely. This not only safeguards against fraudulent activities but also instills confidence in the validity of certifications issued by educational institutions.[25]

In the rapidly evolving landscape of education and professional development, the need for a robust and reliable certification process cannot be overstated. Traditional paper-based certificates, while widely used, are susceptible to various risks, including loss, damage, and manipulation. These vulnerabilities undermine the credibility of academic qualifications and pose

significant challenges for individuals, institutions, and employers alike. By transitioning to a digital certificate system built on blockchain technology, these inherent weaknesses can be effectively addressed, ushering in a new era of trust and transparency in credential verification.[26]

One of the key advantages of blockchain-based digital certificates is their immutability. Once recorded on the blockchain ledger, certificates become tamper-proof and resistant to unauthorized modifications. This not only safeguards the integrity of academic credentials but also enhances their longevity and reliability. Individuals can have greater confidence in the authenticity of their certificates, knowing that they are securely stored on a decentralized and immutable platform.[27]

Moreover, the use of smart contracts enhances the security and transparency of the certification process by automating verification procedures. Smart contracts execute predefined actions automatically once certain conditions are met, eliminating the need for manual intervention and reducing the risk of human error or manipulation. This ensures a streamlined and efficient verification process, saving time and resources for both certificate issuers and verifiers while enhancing the overall reliability of the certification ecosystem.

Furthermore, the integration of QR codes and inquiry string codes onto paper certificates offers a user-friendly and accessible means of verification. Individuals can easily verify the authenticity of their certificates through simple scanning methods, without the need for specialized equipment or technical expertise. This accessibility democratizes the verification process, making it more inclusive and transparent for all stakeholders involved.

Additionally, by reducing the risk of certificate loss or forgery, the proposed digital certificate system addresses longstanding challenges associated with traditional paper-based certificates. Blockchain's decentralized nature ensures that certificates are stored securely and can be accessed from anywhere, at any time, providing a reliable and resilient solution for managing academic credentials in the digital age.

In summary, the adoption of blockchain technology for digital certificates represents a paradigm shift in the certification process, offering enhanced secu-

rity, transparency, and efficiency. By leveraging blockchain's immutable ledger and smart contract capabilities, the proposed system provides a scalable and reliable solution to the challenges posed by traditional paper-based certificates, paving the way for a more trustworthy and accountable certification ecosystem.[28]

CHAPTER 3

METHODOLOGY

3.1 System Architecture and Workflow

The conventional methods of issuing and verifying educational certificates have long been criticized for their inefficiency and susceptibility to fraud. These processes, entrenched in manual labor and paper-based documentation, are not only time-consuming but also prone to errors and manipulation. In response to these challenges, there is a growing demand for a digitalized and streamlined system that can mitigate the risks associated with document forgery.[29]

The proposed solution seeks to address these concerns by harnessing the power of Blockchain technology, specifically leveraging the Ethereum public Blockchain and smart contracts. By digitizing the issuance and verification processes, the system aims to enhance efficiency while bolstering security measures. Through the utilization of IPFS for distributed peer-to-peer storage of documents, the system ensures that educational certificates are securely stored and easily accessible.

One of the key advantages of the proposed system is its ability to offer features such as immutability, decentralization, and tamper-proof documents. By eliminating the reliance on centralized authorities or third-party intermediaries, the system enables direct verification of certificates, thereby reducing the risk of fraud and manipulation.

Central to the system's functionality is the generation of e-certificates with unique hash values, which serve as a basis for certificate verification. This approach ensures the authenticity and integrity of educational credentials, mitigating the vulnerabilities associated with traditional paper-based methods. Moreover, the utilization of Blockchain technology provides a transparent and auditable record of all certificate transactions, further enhancing trust and

accountability in the certification process.

In addition to improving the security and efficiency of certificate issuance and verification, the proposed system offers benefits in terms of accessibility and scalability. With digital certificates stored on the Blockchain, individuals can access and verify their credentials from anywhere in the world, eliminating geographical barriers and streamlining processes for both certificate issuers and recipients.

Overall, the adoption of Blockchain technology in the issuance and verification of educational certificates represents a significant step towards modernizing and securing credentialing processes. By embracing digitalization and leveraging decentralized technologies, the proposed system aims to establish a more reliable and trustworthy framework for managing educational credentials in the digital age.[30]

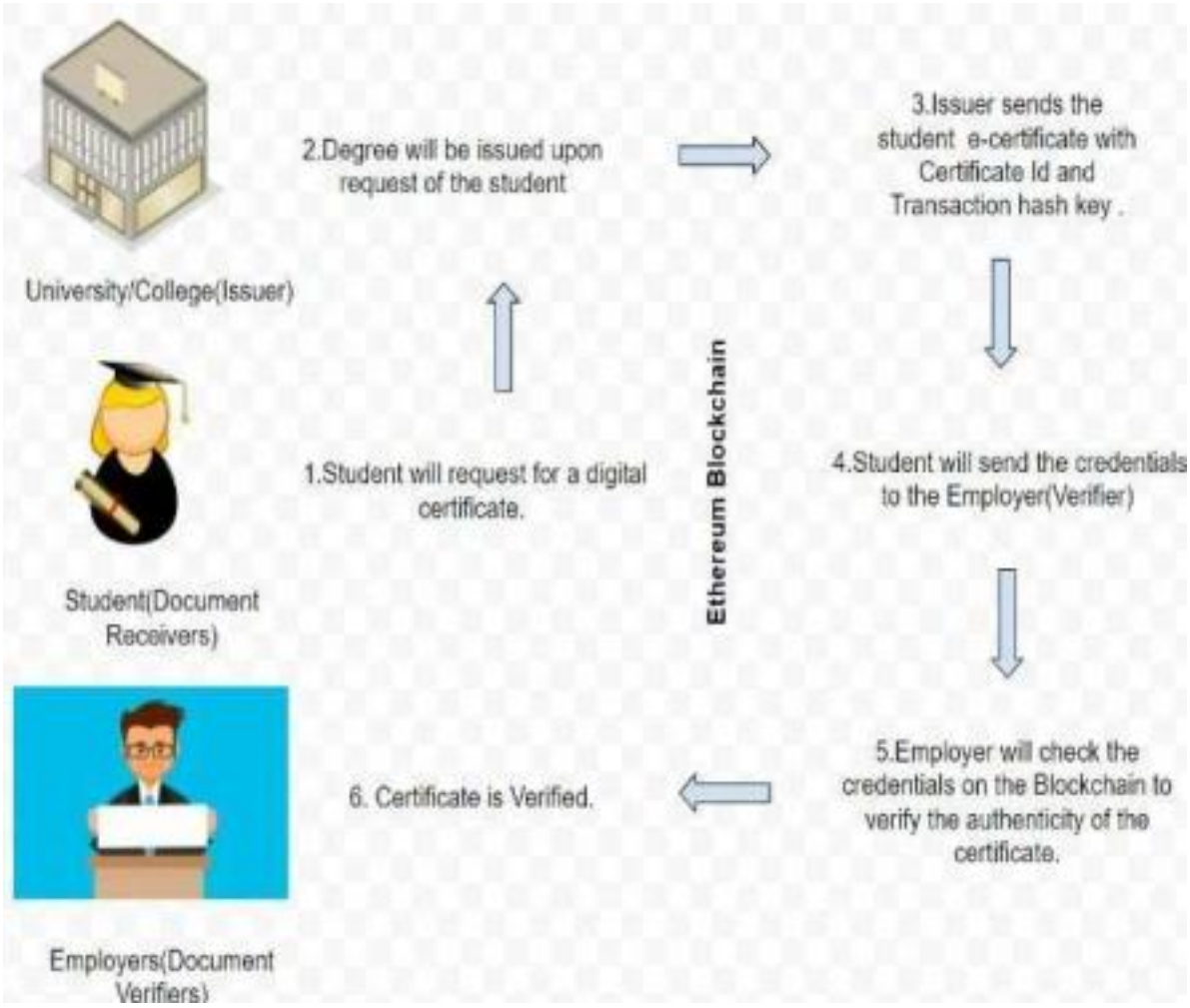

Figure 3.1: System Architecture

As a student, the first step in obtaining a certificate involves registering with your college. This registration process typically involves providing personal information such as your name, student ID, and program of study to the college's administrative office. This information is necessary for the college to verify your identity and eligibility for the certificate you are requesting. Once your registration is complete, you can proceed to request the desired certificate from the college.

After you submit your certificate request, the college acknowledges receipt of your request and begins processing it. This acknowledgment may include confirming your enrollment status, verifying that you have met all necessary requirements for the certificate, and initiating the necessary administrative procedures to generate and issue the certificate. Depending on the college's policies and procedures, this processing time may vary, but you can expect to receive updates on the status of your request as it progresses.

Once the college has processed your certificate request, they will generate an e-certificate containing your credentials. This e-certificate typically includes important details such as your name, the name of the program or course for which the certificate is being awarded, the date of completion, and any relevant academic achievements or distinctions. Importantly, the e-certificate will also contain a unique certificate ID and transaction hash key, which serve as cryptographic identifiers linked to your certificate on the blockchain.

With your e-certificate in hand, you are now able to share it with your employer or any other entity requiring verification of your credentials. When presenting your certificate to your employer, they will utilize blockchain technology to verify its authenticity. This verification process involves accessing the blockchain ledger, where all certified credentials are securely stored. By inputting the unique certificate ID and transaction hash key provided on your e-certificate, your employer can validate the authenticity of your credentials directly from the blockchain.

Once your employer has successfully verified the authenticity of your certificate using blockchain technology, your certificate is considered valid and can be accepted as proof of your qualifications. This verification process is

efficient and reliable, as it leverages the immutable and transparent nature of blockchain technology to ensure the integrity and authenticity of your credentials. As a result, you can confidently present your certificate knowing that it has been verified through a secure and trustworthy system.

3.2 User Interface (UI) Design

The proposed certificate issuance and verification system leverages blockchain technology, Flask for frontend development, IPFS for storing images and generating hash codes, Ganache as the blockchain network, and Metamask for token wallets. The system comprises three primary user interfaces: employer, student, and university.

In the user interface design, each screen features a clean and intuitive layout to streamline navigation and enhance user experience. For employers, a search functionality is included, allowing them to easily locate and verify specific certificates. This feature expedites the verification process, particularly for employers handling a large volume of verifications.

In the student interface, transparency and communication are prioritized. Students receive real-time notifications at each stage of the certificate issuance process, keeping them informed about the status of their requests. Additionally, a messaging feature allows students to communicate directly with university staff regarding their certificate requests.

The university interface offers robust administrative controls to manage user access and permissions effectively. Administrators have the ability to create and manage user accounts, assign roles, and oversee all certificate issuance activities. Comprehensive reporting and analytics capabilities enable administrators to track key metrics such as request volume and processing times.

Overall, the user interface design prioritizes accessibility, ensuring that all users can easily navigate and interact with the system. Clear instructions and tooltips guide users through each step of the certificate issuance and verification process. Additionally, the UI is optimized for various devices and screen sizes to accommodate diverse user preferences and workflows.

The system aims to revolutionize the certificate issuance and verification process by digitizing traditional methods, enhancing efficiency, and bolstering security. By incorporating user-centric design principles, robust functionality, and accessibility features, the UI empowers stakeholders to manage digital certificates seamlessly while maintaining the highest standards of security and integrity.

In addition to the core functionality outlined above, the user interface design also incorporates advanced features to further enhance the user experience and optimize system performance.

One such feature is the integration of multi-factor authentication (MFA) for added security. By requiring users to authenticate their identity through multiple verification methods, such as passwords, biometrics, or one-time passcodes, the system ensures that only authorized individuals can access sensitive information and perform critical actions, such as issuing or verifying certificates.

Furthermore, the user interface includes customizable dashboard views for each user role, allowing individuals to tailor their interface based on their specific preferences and workflow requirements. This flexibility enables users to prioritize the information and tasks most relevant to their responsibilities, improving productivity and efficiency.

Another notable aspect of the UI design is its focus on accessibility and inclusivity. The interface adheres to industry best practices for web accessibility, ensuring that users with disabilities can fully participate in the certificate issuance and verification process. This includes features such as keyboard navigation, screen reader compatibility, and adjustable font sizes and color contrasts.

To enhance collaboration and communication among users, the interface integrates real-time messaging and notification functionalities. Users can communicate securely within the platform, share updates on certificate requests or verifications, and receive alerts for important events or deadlines. This fosters transparency and accountability throughout the process, reducing delays and misunderstandings.

Overall, the user interface design is built on a foundation of usability,

security, and compliance, offering a seamless and intuitive experience for all stakeholders involved in the certificate issuance and verification process. By leveraging cutting-edge technologies and user-centered design principles, the system sets a new standard for digital certificate management in the education sector.

3.3 Data Flow Diagram

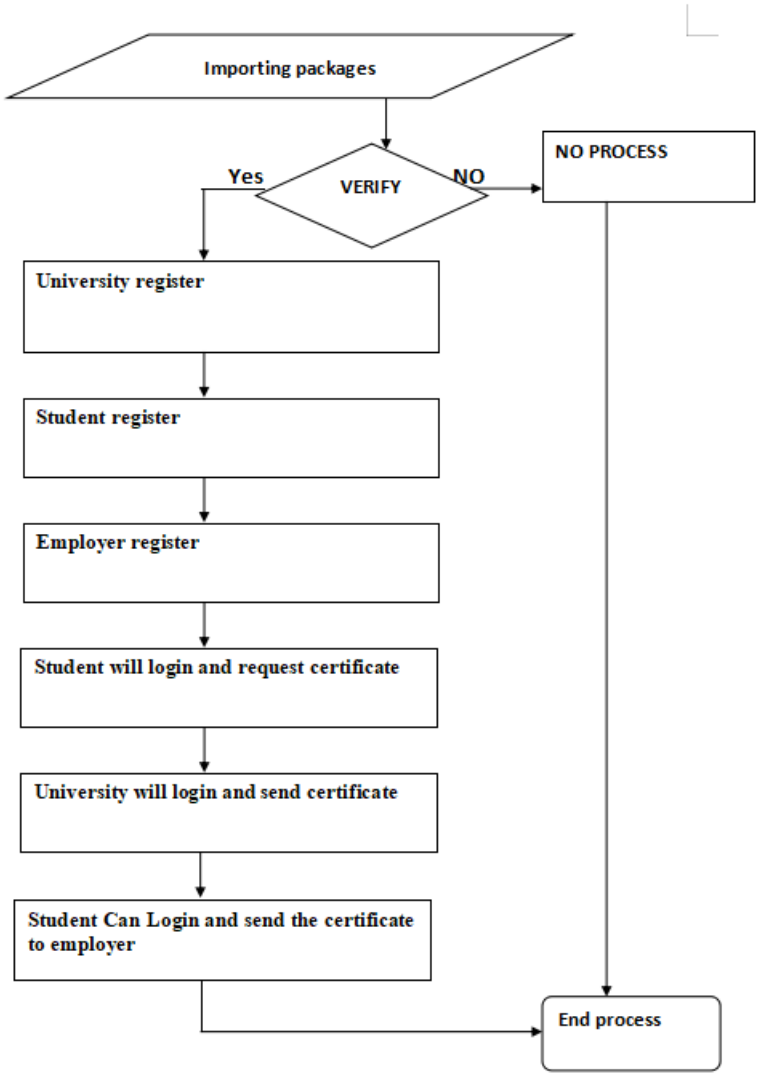

Figure 3.2: Dataflow diagrams

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated

by this system.

The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

3.4 UML Diagrams

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS: The Primary goals in the design of the UML are as follows: 1.Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.

2.Provide extendibility and specialization mechanisms to extend the core concepts. 3.Be independent of particular programming languages and development process.

4.Provide a formal basis for understanding the modeling language.

5.Encourage the growth of OO tools market.

6.Support higher level development concepts such as collaborations, frameworks, patterns and components.

7.Integrate best practices.

3.4.1 Use case diagram

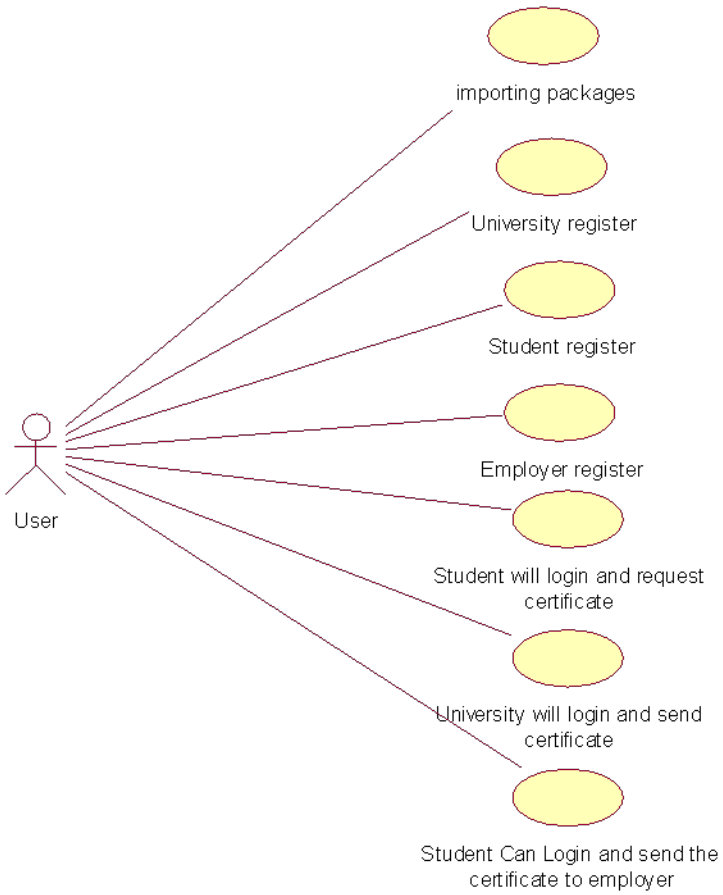

Figure 3.3: Usecase diagram

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by

a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

3.4.2 Class diagram

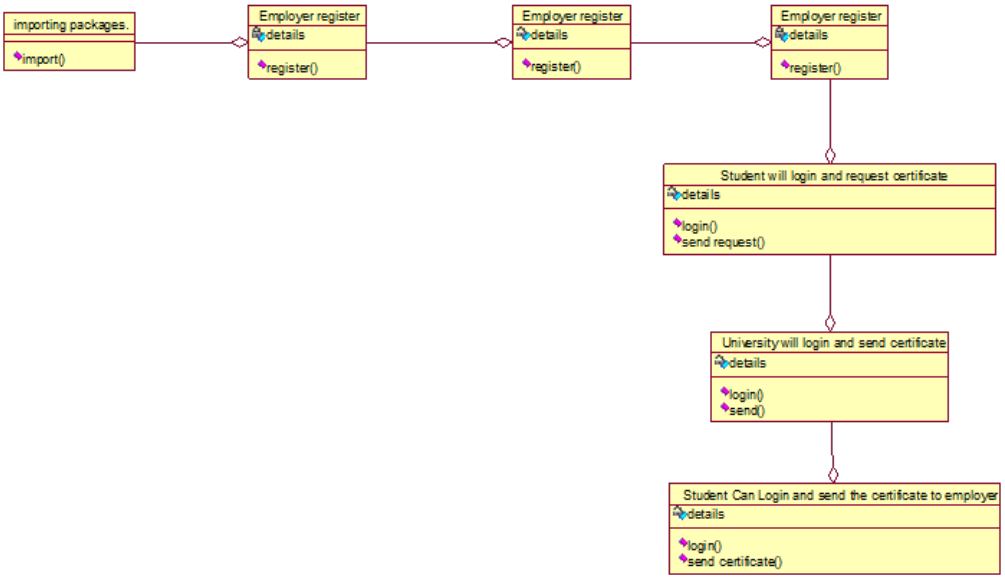

Figure 3.4: Class diagram

The class diagram is used to refine the use case diagram and define a detailed design of the system. The class diagram classifies the actors defined in the use case diagram into a set of interrelated classes. The relationship or association between the classes can be either an ”is-a” or ”has-a” relationship. Each class in the class diagram may be capable of providing certain functionalities. These functionalities provided by the class are termed ”methods” of the class. Apart from this, each class may have certain ”attributes” that uniquely identify the class.

3.4.3 Activity diagram

The process flows in the system are captured in the activity diagram. Similar to a state diagram, an activity diagram also consists of activities, actions, transitions, initial and final states, and guard conditions.

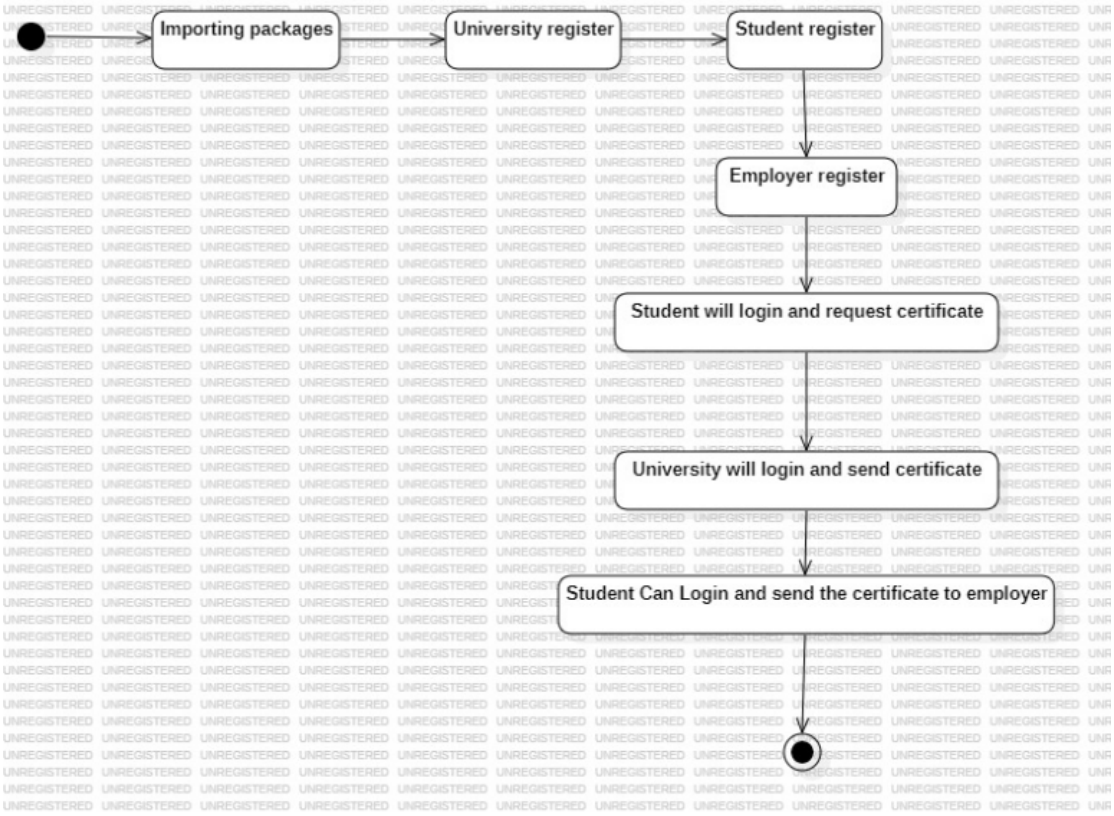

Figure 3.5: Activity diagram

3.4.4 Sequence diagram

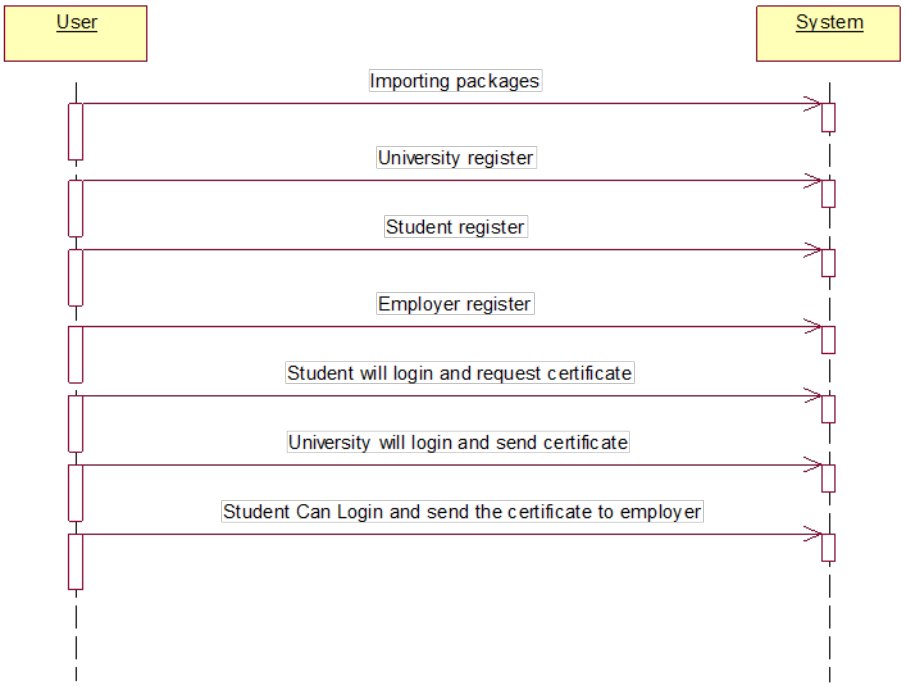

Figure 3.6: Sequence diagram

A sequence diagram represents the interaction between different objects in the system. The important aspect of a sequence diagram is that it is time-ordered. This means that the exact sequence of the interactions between the objects is represented step by step. Different objects in the sequence diagram interact with each other by passing "messages".

3.4.5 Collaboration diagram

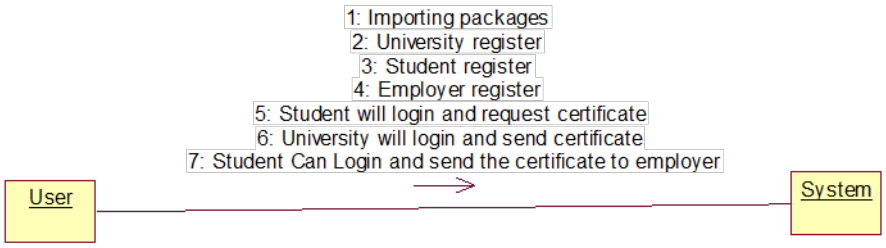

Figure 3.7: Collaboration diagram

A collaboration diagram groups together the interactions between different objects. The interactions are listed as numbered interactions that help to trace the sequence of the interactions. The collaboration diagram helps to identify all the possible interactions that each object has with other objects.

3.4.6 Component diagram

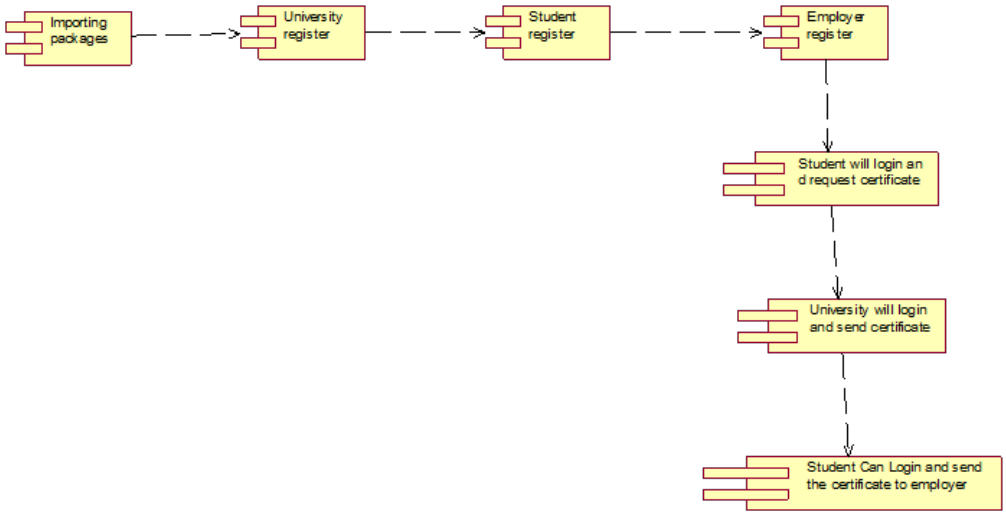

Figure 3.8: Component diagram

The component diagram represents the high-level parts that make up the system. This diagram depicts, at a high level, what components form part of the system and how they are interrelated. A component diagram depicts the components culled after the system has undergone the development or construction phase.

3.4.7 Deployment diagram

Figure 3.9: Deployment diagram

The deployment diagram captures the configuration of the runtime elements of the application. This diagram is by far most useful when a system is built and ready to be deployed.

CHAPTER 4

IMPLEMENTATION

4.1 Development of User Interface

The blockchain utilized in this system is Ethereum, known for its decentralized and permissionless nature. Ethereum offers a robust platform for executing smart contracts, facilitating secure transactions, and storing immutable data. However, due to the inherent size limitations of public blockchains like Ethereum, the system adopts a hybrid approach by storing hash values of certificates on the blockchain within transactions, while the actual certificates are stored on IPFS (InterPlanetary File System). This combination ensures efficient storage and retrieval of certificate data while leveraging the security and transparency of blockchain technology.

Smart contracts, developed using Solidity, Ethereum's native programming language, play a crucial role in automating and enforcing the certificate issuance and verification process. These smart contracts govern the rules and conditions for issuing, transferring, and verifying certificates, ensuring trust and integrity throughout the system.

The certificate issuance process begins with universities or colleges, acting as issuers, logging into a central platform to create digital certificates for students. Each certificate is assigned a unique Certificate ID and Transaction hash value, which serves as a digital fingerprint for authentication purposes. This ensures the uniqueness and integrity of each certificate, preventing tampering or forgery.

Verifiers, such as employers or academic institutions, can then authenticate certificates using either the Certificate ID or Transaction hash value. This streamlined verification process eliminates the need for manual verification procedures, saving time and resources for both issuers and verifiers. Moreover, the use of blockchain technology enhances the security and reliability of certificate verification, mitigating the risk of fraud or manipulation.

The proposed system caters to three main types of users: Issuers (universities/colleges), Document/degree receivers (students), and Document verifiers (employers). Issuers are responsible for generating digital certificates based on student details, providing a unique Certificate ID and Transaction hash value to each student. Students, as document receivers, receive their e-certificates containing the Certificate ID/IPFS hash and Transaction hash value, ensuring secure and tamper-proof delivery of certificates.

Document verifiers, such as employers or academic institutions, can swiftly verify certificate authenticity using either the Certificate ID or Transaction Hash, enhancing the efficiency of the verification process. This seamless verification mechanism enables employers to validate the credentials of job applicants quickly and accurately, streamlining the hiring process and ensuring the integrity of the workforce.

The initial user, known as the Document Issuer, gathers student information like name, college ID, and course name. This data is then submitted on a designated platform, enabling the Issuer to establish a user profile for the student, who acts as the Document Receiver. Additionally, the Issuer digitally signs the certificate and stores it within a Document Management System (IPFS), while recording its hash value on the Blockchain. This profile serves as a centralized repository for all of the student's certificates, facilitating easy access and management.

Subsequently, an E-certificate can be shared with Document Verifiers for verification purposes, ensuring seamless and secure credential verification. This innovative approach to certificate issuance and verification leverages the power of blockchain technology to enhance transparency, security, and efficiency in the education sector, paving the way for a more reliable and trustworthy certification process.

4.2 Testing Strategies

Unit testing is an integral part of the software development process, focusing on testing individual modules to ensure their functional correctness. It involves isolating each unit of the system to identify and fix defects, typically conducted

by the developer themselves. The two primary techniques used in unit testing are Black Box Testing and White Box Testing. Black Box Testing evaluates the user interface, input, and output of the system without considering its internal workings, while White Box Testing examines the internal behavior of functions within the modules to ensure their correctness.

Data flow testing is another important strategy that involves selecting paths through the program's control flow to explore the sequence of events related to the status of variables or data objects. This testing focuses on points where variables are received and where these values are used, ensuring the integrity of data flow within the system. Integration testing, conducted after unit testing, verifies the functional, performance, and reliability aspects between the integrated modules. One approach to integration testing is Big Bang Integration Testing, where all units are linked at once to create a complete system.

User interface testing is crucial for identifying defects in a product's graphical user interface (GUI), ensuring usability, accessibility, and functionality. This testing technique focuses on enhancing the overall user experience by ensuring the GUI's usability and functionality.

Test cases play a crucial role in ensuring the robustness and reliability of the system. For instance, in the case of registering a user, the expected outcomes include successful registration if the process is available and no registration process initiation if it is not available. Similarly, for login functionality, successful login should be possible if the feature is available, while absence of login functionality would prevent successful login attempts.

Data flow testing involves testing various data inputs to ensure proper flow between variables and data objects, while integration testing verifies the interactions between integrated modules. Big Bang Integration Testing aims to create a complete system by linking all units simultaneously, whereas user interface testing focuses on identifying defects in the GUI to enhance user experience. Overall system testing encompasses comprehensive testing of all components and functionalities to identify and resolve defects, ensuring system reliability and performance.

4.2.1 Test Cases

Test cases play a crucial role in ensuring the effectiveness and reliability of a system. They provide a systematic approach to verifying whether the system functions as intended and meets the specified requirements. Here are some test cases for the system:

1. For the registration process, a test case involves submitting registration details. The expected outcome is a successful registration with a confirmation message if the process is available. However, if the registration process is unavailable, there should be no initiation of the registration process, and an error message indicating its unavailability should be displayed.

2. Another critical test case is for the login functionality. In this scenario, users enter valid login credentials. The expected outcome is a successful login with access to the system's features if the login process is available. Conversely, if the login functionality is inaccessible, the system should prevent successful login attempts and display an error message.

3. Processing requests is a fundamental aspect of the system. A test case for this scenario involves users submitting a request for processing. If the processing capability is available, the expected outcome is the successful processing of the request, accompanied by a confirmation message. However, if processing is unavailable, the system should not initiate the processing and display an error message indicating its unavailability.

4. Data flow testing is essential to ensure the proper flow of data between variables and data objects, maintaining integrity and consistency within the system. This involves providing various data inputs to the system and verifying that the data flows correctly through the system's components.

5. Integration testing evaluates the interactions between integrated modules within the system. Test cases for integration testing involve verifying functional, performance, and reliability aspects between integrated modules to ensure seamless operation.

6. Big Bang Integration Testing assesses the integration of all units simultaneously to create a complete system. Test cases for this scenario focus on identifying any errors or issues resulting from the integration of all units

at once.

7. User interface testing involves interacting with the graphical user interface (GUI) to identify defects or inconsistencies. Test cases in this category aim to ensure the usability and functionality of the GUI by thoroughly evaluating its responsiveness and user experience.

These test cases cover various aspects of the system, including registration, login, request processing, data flow, integration, and user interface testing. By executing these test cases, the system's reliability, functionality, and adherence to requirements can be thoroughly evaluated and validated.

CHAPTER 5

Results

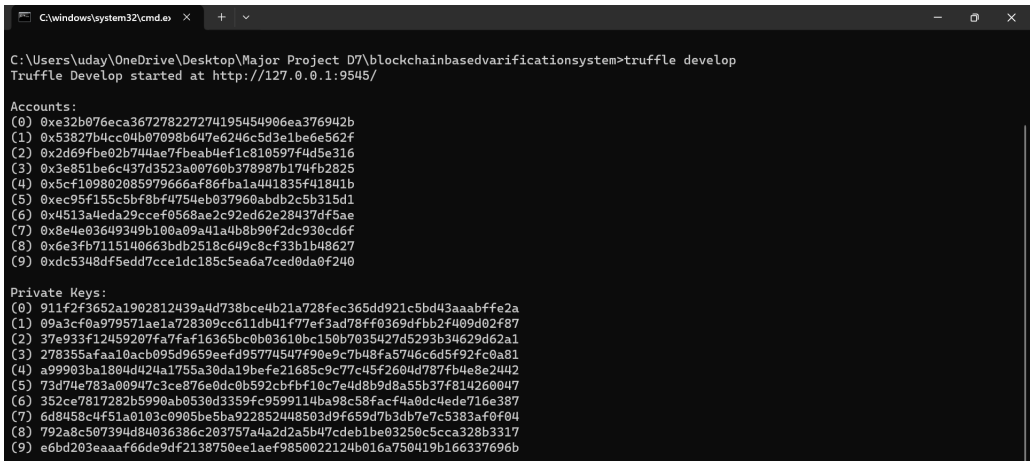

Figure 5.1: Hosting blockchain on localhost

Hosting a blockchain on the localhost using Truffle involves setting up a local Ethereum network for development and testing purposes. Truffle provides a convenient framework for compiling, migrating, and interacting with smart contracts, making it an ideal choice for blockchain development. By configuring Truffle to connect to a local network and deploying contracts using migration scripts, developers can efficiently develop and test decentralized applications (DApps) in a controlled environment before deploying them to a production network.

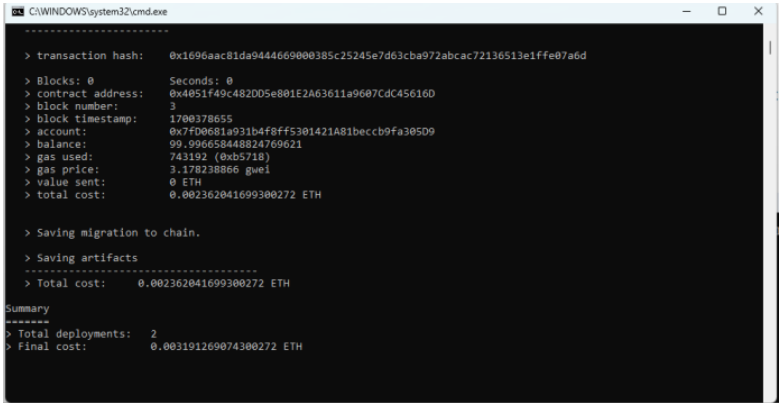

Figure 5.2: Compiling smart contract file

Compiling a smart contract file is a crucial step in the process of developing decentralized applications (DApps) on a blockchain network. This process involves translating the human-readable Solidity code into bytecode, which can be executed by the Ethereum Virtual Machine (EVM). By using a Solidity compiler like solc, developers can ensure that their smart contracts are correctly translated into machine-readable bytecode, ready for deployment on the blockchain. Additionally, modern development frameworks like Truffle provide built-in functionality for compiling smart contracts, streamlining the development process and ensuring compatibility with the chosen blockchain network. Once compiled, the smart contract bytecode is ready to be deployed to the blockchain, where it will be executed as part of the decentralized application's logic.

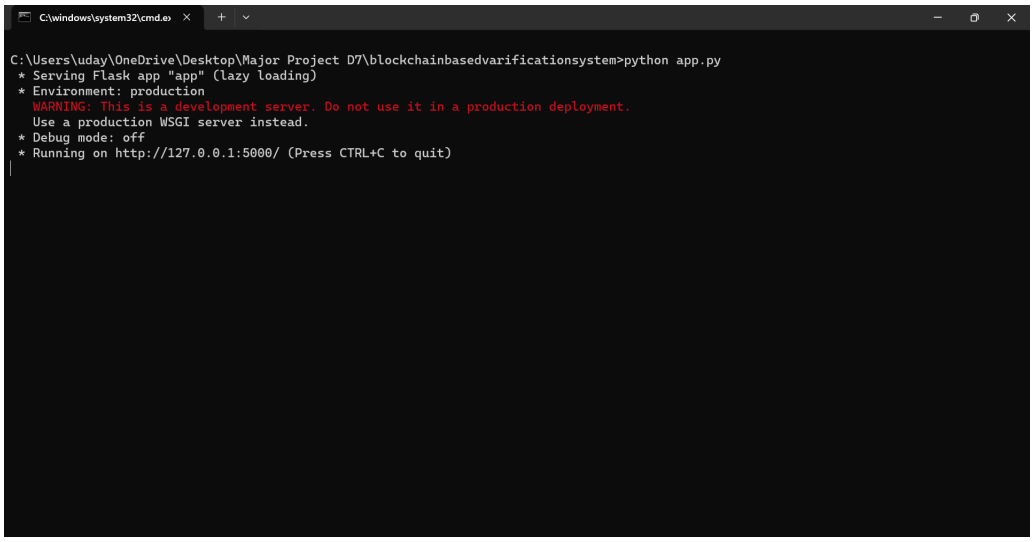

Figure 5.3: Hosting Flask Server

Hosting a Flask server is a fundamental aspect of deploying web applications built using the Flask framework. Flask, a lightweight and flexible Python web framework, allows developers to create dynamic and interactive web applications with ease. When hosting a Flask server, developers typically choose a suitable hosting provider or server environment to deploy their Flask application. This could range from traditional web hosting services to cloud platforms like AWS, Google Cloud Platform, or Heroku.

To host a Flask server, developers need to ensure that their server environment meets the necessary requirements for running Python applications and

Flask frameworks. This often involves configuring the server environment with the required dependencies, such as Python and Flask libraries, and setting up a WSGI server to handle incoming requests.

Once the server environment is set up, developers can deploy their Flask application by transferring the application files to the server and configuring the server to run the Flask application. This may involve setting up routes, defining endpoints, and configuring any necessary middleware or plugins.

Overall, hosting a Flask server involves setting up a suitable server environment, deploying the Flask application to the server, and configuring the server to handle incoming requests and serve the Flask application to users. By following these steps, developers can successfully host their Flask applications and make them accessible to users over the internet.

Figure 5.4: University Registration

University registration on the blockchain is a foundational step towards establishing the institution's presence within the decentralized network. This process begins with the submission of essential credentials, including the university's name, username, password, address, and contact number. Each piece of information plays a crucial role in verifying the institution's identity and facilitating secure interactions within the blockchain ecosystem. Once registered, the university gains access to a range of blockchain functionalities, empowering it to issue and verify academic credentials, engage in transparent transactions, and foster trust and accountability within the academic community.

The registration process underscores the significance of accurate and ver-

ified information, ensuring the integrity and authenticity of the university's identity within the blockchain network. By providing comprehensive credentials, universities demonstrate their commitment to transparency, security, and innovation in credentialing practices. Moreover, registration on the blockchain opens doors to new opportunities for collaboration, research, and data management, positioning universities at the forefront of digital transformation in the education sector.

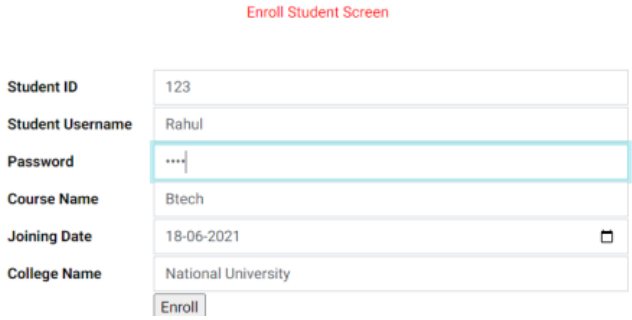

Figure 5.5: Student Registration

Student registration on the blockchain involves the submission of essential credentials, including the student ID, username, password, course name, joining date, and college name. Each piece of information serves to authenticate the student's identity and academic affiliation within the blockchain network. By providing accurate and verified credentials, students gain access to a range of blockchain-enabled services and functionalities, including secure storage of academic records, streamlined verification processes, and enhanced data privacy.

The registration process ensures the integrity and transparency of student information within the blockchain ecosystem, fostering trust and accountability in academic transactions. With blockchain technology, students can securely manage their academic credentials, track their educational journey, and seamlessly share verified records with academic institutions and prospective employers. By embracing blockchain-based registration systems, students position themselves at the forefront of digital innovation in education, leveraging decentralized technologies to enhance the credibility and accessibility of

their academic achievements.

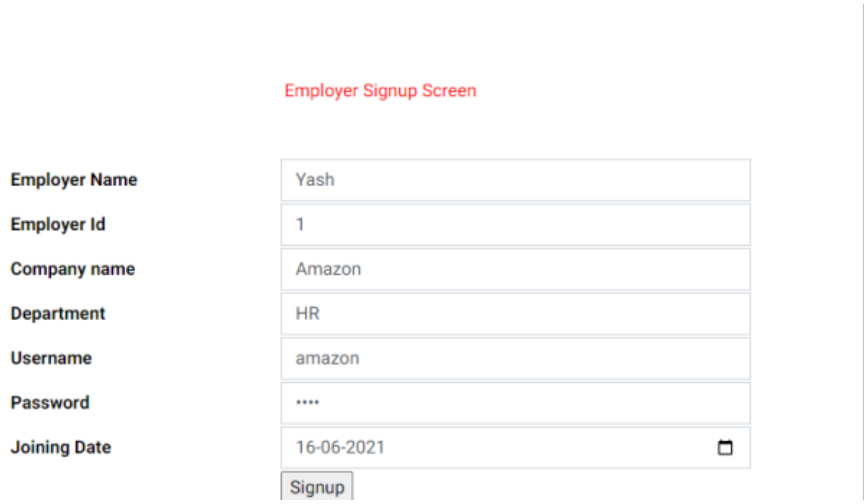

Figure 5.6: Employee Registration

Employee registration within the blockchain network involves the submission of essential credentials, including the employer's name, ID, company name, department, username, password, and joining date. Each piece of information serves to authenticate the employer's identity and professional affiliation within the blockchain ecosystem. By providing accurate and verified credentials, employers gain access to a range of blockchain-enabled services and functionalities, including secure storage of employment records, streamlined verification processes, and enhanced data privacy.

The registration process ensures the integrity and transparency of employer information within the blockchain network, fostering trust and accountability in professional interactions. With blockchain technology, employers can securely manage their employment credentials, track their professional journey, and seamlessly share verified records with relevant stakeholders. By leveraging blockchain-based registration systems, employers embrace digital innovation in human resources management, utilizing decentralized technologies to enhance the credibility and reliability of their professional profiles.

Student login and certificate request functionalities streamline the academic credentialing process within the blockchain network. Upon logging into the system with their unique credentials, students gain access to a range of features tailored to their academic journey. From the user dashboard, students can initiate certificate requests by providing necessary details such as their student

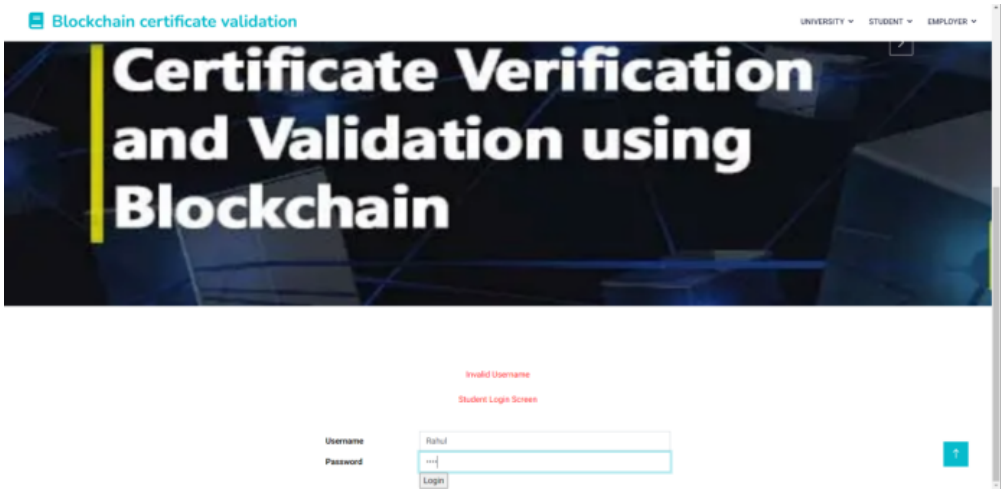

Figure 5.7: Student login

ID, course name, joining date, and college name. This streamlined process eliminates the need for manual paperwork and accelerates the issuance of digital certificates, enhancing the efficiency of academic credential management.

By integrating blockchain technology into the student login and certificate request process, universities and educational institutions ensure the security and integrity of academic records. Each certificate request is securely recorded on the blockchain ledger, providing an immutable and transparent record of student achievements. Through blockchain-enabled systems, students can conveniently request certificates, track the status of their requests, and securely access their digital credentials, empowering them to navigate their academic journey with confidence and ease.

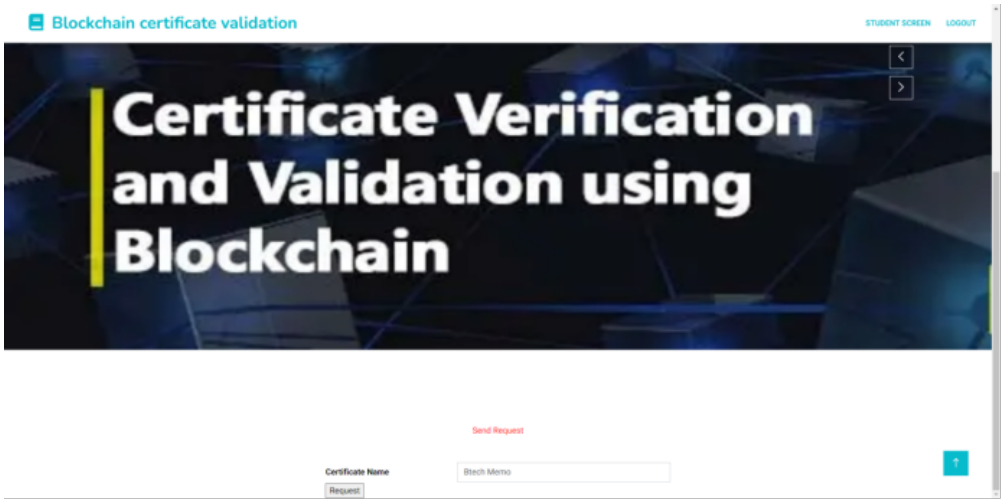

Figure 5.8: Certificate Details

In the certificate details section, students are prompted to enter the name

of the certificate they are requesting. This step ensures that the certificate is accurately identified and generated according to the student's academic achievements. By specifying the certificate name, students can ensure that the digital credential they receive reflects their educational accomplishments with precision and clarity, facilitating seamless verification and recognition of their qualifications.

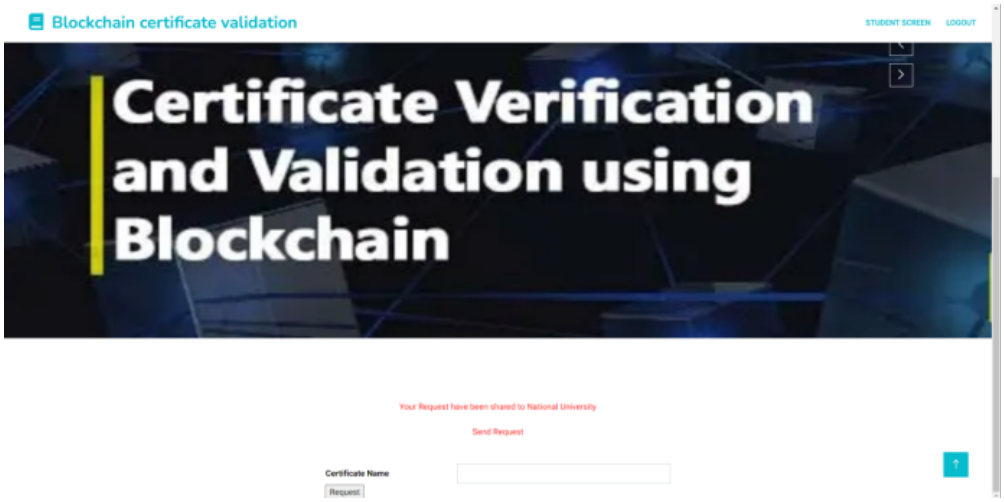

Figure 5.9: Certificate Shared

After clicking "Send," the system initiates the process of sharing the certificate with the designated university representative. Upon successful transmission, a confirmation message is displayed, indicating that the certificate has been shared with the respective university. This notification assures students that their certificate request has been successfully communicated to the university's administrative department for processing and validation.

Figure 5.10: University login

When logging in, the university representative is directed to the requested screen, where they can view incoming certificate requests from students. This screen displays a list of pending requests, providing essential details such as student ID, certificate type, and request date. The interface is designed to facilitate efficient processing of requests, allowing university staff to review and respond to each request promptly. By accessing this screen, universities can manage certificate requests effectively, ensuring timely verification and issuance of academic credentials.

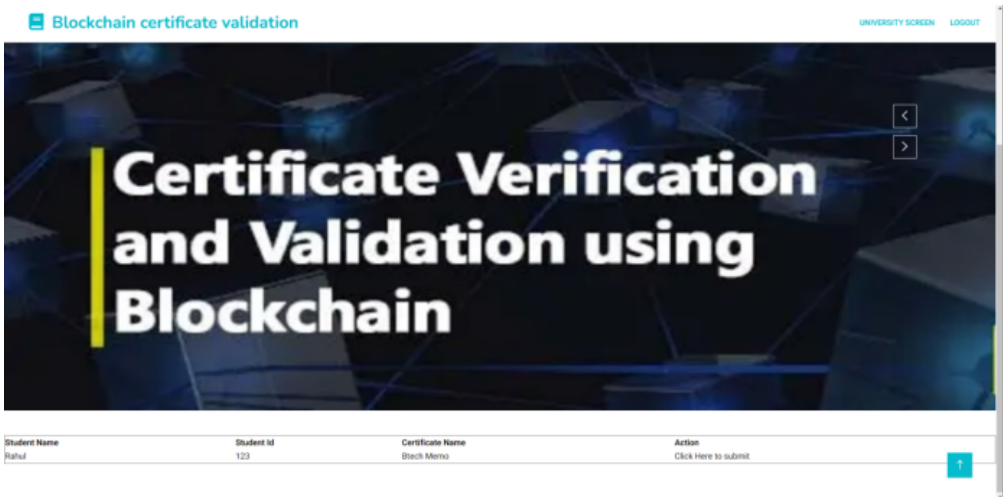

Figure 5.11: University sees request

Upon reviewing the certificate request, the university representative can take action by clicking on the "Submit" button provided on the interface. This action signifies the university's response to the student's request, indicating whether the requested certificate will be granted or denied. By clicking the "Submit" button, the university finalizes its decision and updates the status of the request accordingly within the system. This user-friendly interface simplifies the administrative process for universities, allowing them to efficiently manage certificate requests and respond promptly to student inquiries.

To upload the requested certificate, the university representative navigates through the system to locate the appropriate file containing the certificate. Once found, the representative clicks on the designated "Browse" button or similar functionality provided on the interface. This action opens a file explorer window, allowing the user to select the desired certificate file from their local storage or network. After selecting the file, the university representative

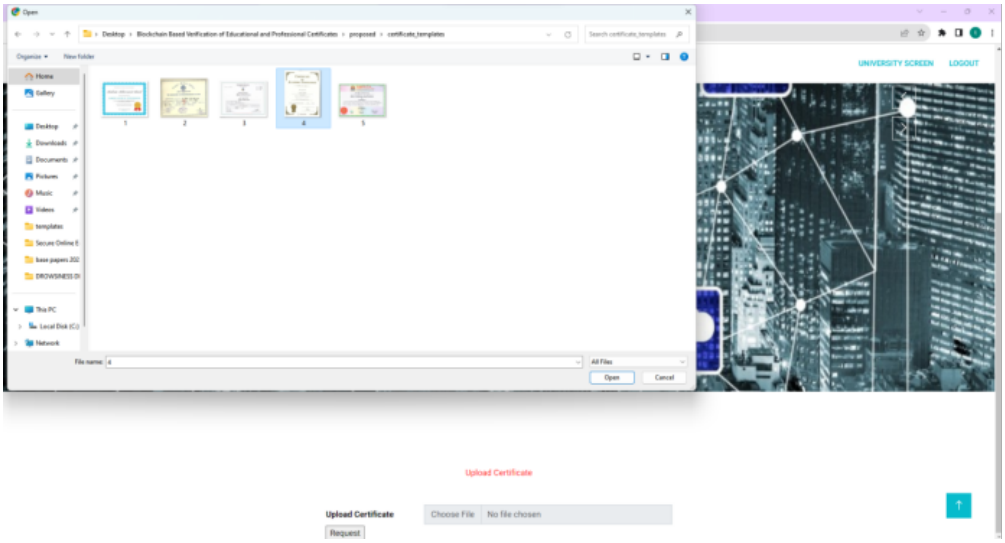

Figure 5.12: University Browse Certificate

confirms the upload by clicking on the "Upload" or "Submit" button, depending on the interface design. This seamless process ensures that the requested certificate is securely uploaded and attached to the student's request within the system, facilitating efficient document management and verification.

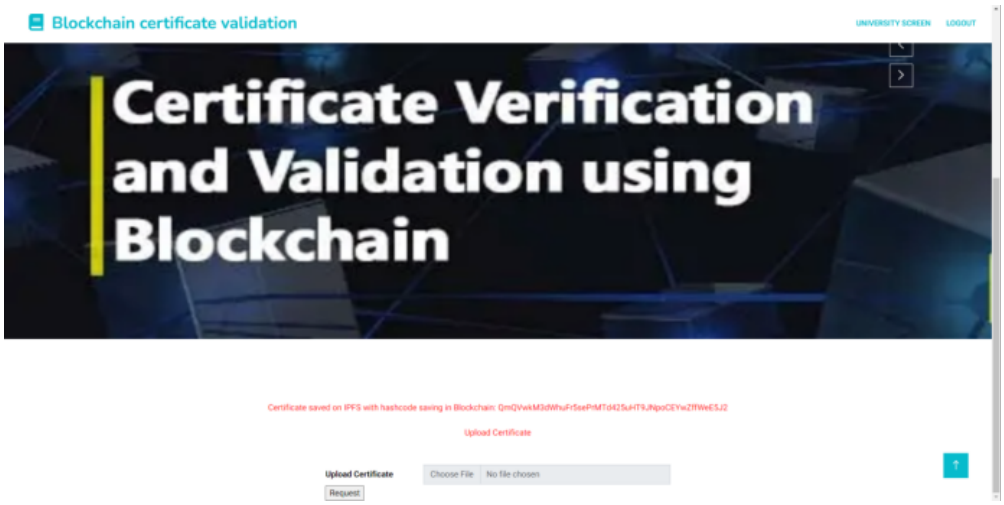

Figure 5.13: University Shared Certificate

Upon successful upload, the university initiates the process of sharing the certificate with the student. The system automatically stores the certificate image on the InterPlanetary File System (IPFS), a decentralized storage protocol known for its reliability and security. Subsequently, the system generates a unique hash code for the uploaded certificate image, which serves as a reference linked to the blockchain. This hash code, along with relevant metadata, is securely stored on the blockchain, ensuring the immutability and

integrity of the certificate data.

Simultaneously, the university system sends a notification to the student, informing them that their requested certificate is now available for access. Depending on the system's configuration, the notification may be delivered through email, SMS, or an in-app notification. The student can then log in to their account and navigate to the designated section to view and download the shared certificate. This streamlined process ensures efficient communication and collaboration between the university and the student while maintaining the security and authenticity of the certificate data stored on the blockchain.

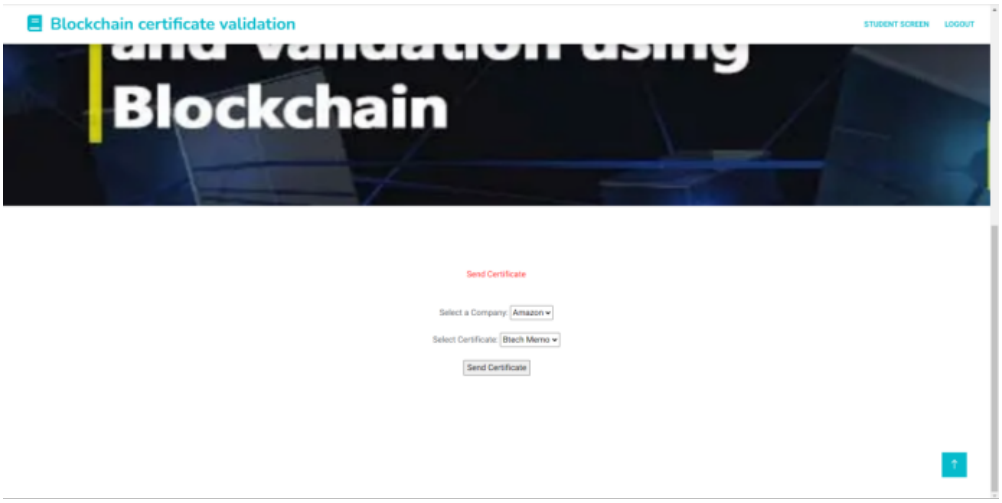

Figure 5.14: Student Sending Certificate to Employer

Once logged in, the student can navigate to the "Certificate Sharing" section of the user interface, where they can initiate the process of sending their certificate to an employer. In this section, the student is prompted to provide the necessary details, such as the employer's name, email address, and any additional message or note they wish to include along with the certificate. Upon entering the required information, the student can proceed to upload the certificate file from their local device or select a previously shared certificate from their account.

After selecting the certificate to be shared, the student simply clicks on the "Send Certificate" button to initiate the sharing process. The system then securely transmits the certificate file to the specified employer via the provided email address. Additionally, the system records this transaction on the blockchain, ensuring transparency and traceability of the certificate-sharing

activity. This streamlined process enables students to efficiently share their academic credentials with prospective employers, facilitating the job application and recruitment process.

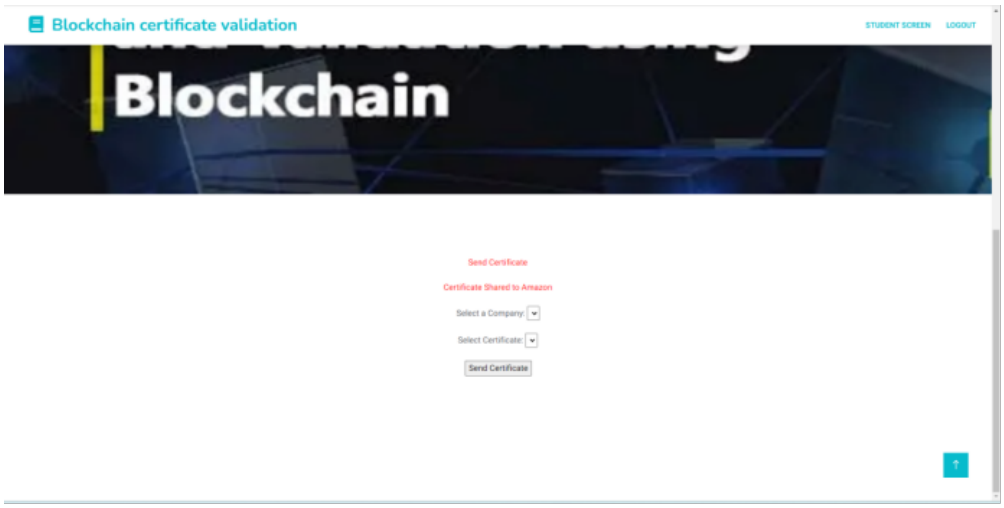

Figure 5.15: Certificate Shared with Employer

Once the student initiates the sharing process, the certificate is securely transmitted to the specified employer. The employer receives an email notification containing a link to access the shared certificate through the platform. Upon clicking the link, the employer is directed to a secure webpage where they can view and download the certificate file.

Simultaneously, the system records the sharing transaction on the blockchain, capturing details such as the sender (student), recipient (employer), timestamp, and hash of the shared certificate. This ensures a transparent and auditable record of the certificate-sharing activity, bolstering the integrity and trustworthiness of the credential verification process. By leveraging blockchain technology, the system provides a tamper-proof and verifiable record of certificate sharing, enhancing the security and reliability of academic credentials in the digital realm.

After logging in, the employer gains access to the platform's dashboard, where they can navigate to the "Certificates" section to view the certificates shared by students. The certificates screen displays a list of all certificates received by the employer, along with relevant details such as the student's name, course completion date, and the issuing university. Each certificate entry is accompanied by options to download the certificate file or view its

Figure 5.16: Employer Login

details.

Employers can conveniently review and verify the authenticity of the shared certificates directly through the platform. By providing a user-friendly interface and comprehensive certificate management features, the system streamlines the verification process for employers, enabling them to efficiently validate the credentials of job applicants or current employees.

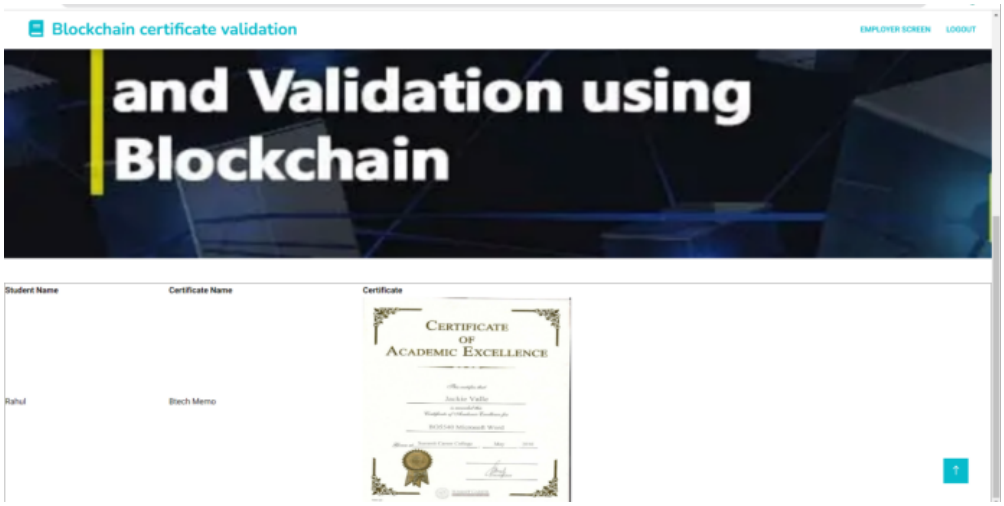

Figure 5.17: Certificate Shared by Student

Once the employer accesses the certificate shared by the student, the system initiates the verification process. Initially, the hash code provided by the student is cross-referenced with the corresponding hash stored on the blockchain. This ensures the integrity and authenticity of the certificate data, as any discrepancy in the hash codes would indicate tampering or unauthorized modifications.

Following the blockchain verification, the system retrieves the IPFS hash associated with the certificate. This IPFS hash serves as a unique identifier for locating the certificate image stored on the decentralized IPFS network. The system retrieves the certificate image using the IPFS hash and securely loads it onto the employer's screen for review.

By leveraging blockchain technology and IPFS storage, the system ensures a robust and tamper-proof verification process for certificates shared by students. Employers can confidently verify the authenticity of certificates, knowing that the data has been securely stored and validated through decentralized mechanisms. This streamlined process enhances trust and reliability in the certification ecosystem, benefiting both employers and students alike.

In this project, we've developed a comprehensive blockchain-based system for efficient issuance and verification of educational certificates. Leveraging technologies like Ethereum, IPFS, Flask, and Truffle, we've created a robust platform that ensures the integrity and authenticity of academic credentials. From university registration to certificate sharing between students, employers, and universities, each step in the process is meticulously designed to streamline operations and enhance security.

Through this system, students can seamlessly request, receive, and share their certificates, while employers can efficiently verify the authenticity of these credentials. With blockchain serving as the underlying infrastructure, users can trust in the validity and integrity of the certificates, thus mitigating the risk of fraud and ensuring a reliable certification process for all stakeholders involved.

CHAPTER 6

Conclusions and Future Scope

The proposed blockchain-based system for certificate issuance and verification offers a robust solution to address the shortcomings of traditional methods in the education sector. By harnessing the power of blockchain technology, the system ensures the authenticity and integrity of academic credentials while streamlining the verification process. The use of unique hash values for each certificate enhances security and reduces the risk of fraud, instilling confidence in stakeholders.

6.1 Summary of findings

The summary of findings highlights the transformative impact of blockchain technology on certificate issuance and verification processes in the education sector. Through the implementation of blockchain-based systems, the cumbersome and time-consuming nature of traditional paper-based methods is effectively mitigated. This streamlining of processes not only improves efficiency but also reduces the risk of errors and fraud, enhancing overall trust and confidence in academic credentials.

Furthermore, the tamper-proof nature of blockchain ensures the integrity and authenticity of certificates, providing a secure and transparent platform for verification. By leveraging unique hash values for each certificate, the system creates a verifiable record that is resistant to tampering or manipulation, thereby safeguarding against fraudulent activities. This level of security and reliability is crucial for maintaining the credibility of academic qualifications and protecting the interests of stakeholders.

Moreover, the adoption of blockchain technology in certificate management systems opens up new avenues for innovation and collaboration within the education ecosystem. As institutions embrace digital transformation, there is potential for the development of standardized protocols and interoperable

systems that facilitate seamless exchange of credentials across institutions and organizations. This interoperability enhances accessibility and usability, ultimately benefiting students, employers, and educational institutions alike.

In conclusion, the summary of findings underscores the significant advantages offered by blockchain technology in revolutionizing certificate management processes. By addressing the inherent challenges of traditional methods and introducing new levels of security and efficiency, blockchain-based systems pave the way for a more reliable, transparent, and trustworthy certification ecosystem in the digital age.

6.2 Future Scope

In the future, we plan to make the system even better. We'll introduce QR codes, which will make verifying certificates easier. Instead of using long numbers like Certificate IDs, people can just scan the QR code to check if a certificate is real.

Another improvement we're considering is sending credentials directly to students' email addresses. This means students won't have to wait or worry about getting their certificates. Everything will be done automatically, making the process smoother and faster for everyone involved.

REFERENCES

[1] *8 Use Cases Of Blockchain In Education - TruScholar*. https://www.truscholar.io/8-use-cases-of-blockchain-ineducation/. Accessed Jun. 25, 2022.

[2] *The Cost of a Bad Hire to Your Business*. https://resources.careerbuilder.com/recruiting-solutions/howmuch-isthat-badhire-costing-your-business. Accessed Jun. 25, 2022.

[3] *Dean at M.I.T. Resigns*. http://www.nytimes.com/2007/04/27/us/27mit.html. Accessed Jun. 25, 2022.

[4] *Judge Jenny Lind Aldecoa-Delorino v. Marilyn de Castro Remigio-Versoza. A.M. No. P-08-2433., Supreme Court of the Philippines, September 25, 2009*. http://sc.judiciary.gov.ph/jurisprudence/2009/september2009/P-08-2433.html.

[5] G. A. Phillips. "Degree Mills: The Billion-Dollar Industry That Has Sold Over a Million Fake Diplomas by Allen Ezell, John Bear (review)". In: *The Review of Higher Education* 37.2 (2014), pp. 282–284. DOI: 10.1353/RHE.2014.0002.

[6] *University of Nicosia Issues Block-Chain Verified Certificates*. https://www.coindesk.com/markets/2014/09/16/universityofnicosiaissues-block-chain-verified-certificates/. Accessed Jun. 25, 2022.

[7] R. Arenas and P. Fernandez. "CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials". In: *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. 2018. DOI: 10.1109/ICE.2018.8436324.

[8] M. Oliver, J. Moreno, G. Prieto, and D. Benítez. *Using Blockchain as a Tool for Tracking and Verification of Official Degrees: Business Model*. Trento: International Telecommunications Society, 2018.

[9] T. Kanan, A. T. Obaidat, and M. Al-Lahham. "SmartCertBlockChain Imperative for Educational Certificates". In: *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*. 2019, pp. 629–633. DOI: 10.1109/JEEIT.2019.8717505.

[10] J. C. Cheng, N. Y. Lee, C. Chi, and Y. H. Chen. "Blockchain and smart contract for digital certificate". In: *Proceedings of 4th IEEE International Conference on Applied System Innovation 2018 (ICASI2018)*. 2018, pp. 1046–1051. DOI: 10.1109/ICASI.2018.8394455.

[11] A. El-Dorry, M. Reda, S. A. el Khalek, S. El-Din Mohamed, R. Mohamed, and A. Nabil. "Egyptian Universities Digital Certificate Verification Model Using Blockchain". In: *ACM International Conference Proceeding Series*. 2020, pp. 79–83. DOI: 10.1145/3436829.3436864.

[12] T. Nurhaeni, I. Handayani, F. Budiarty, D. Apriani, and P. A. Sunarya. "Adoption of Upcoming Blockchain Revolution in Higher Education: Its Potential in Validating Certificates". In: *2020 Fifth International Conference on Informatics and Computing (ICIC)*. Gorontalo, Indonesia, 2020, pp. 1–5. DOI: 10.1109/ICIC50835.2020.9288605.

[13] S. Nikolić, S. Matić, D. Čapko, S. Vukmirović, and N. Nedić. "Development of a Blockchain-Based Application for Digital Certificates in Education". In: *2022 30th Telecommunications Forum (TELFOR)*. Belgrade, Serbia, 2022, pp. 1–4. DOI: 10.1109/TELFOR56187.2022.9983672.

[14] Paul Attewell and Thurston Domina. "Educational imposters and fake degrees". In: *Research in Social Stratification and Mobility* 29.1 (2011). DOI: 10.1016/j.rssm.2010.12.004.

[15] Inayatulloh. "Blockchain Technology Model to Protect Higher Education E-Certificates with Open Source system". In: *2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS)*. Makasar, Indonesia, 2021, pp. 1–4. DOI: 10.1109/ICORIS52787.2021.9649606.

[16] Dindayal Mahto, Seshanthan Murali, Balamurgan Selvaraj, and Sruthi Arasu. "Decentralized Approach for Graduates' Certificate Generation, Validation, and Verification". In: *2023 IEEE 2nd International Conference on Industrial Electronics: Developments Applications (ICIDeA)*. 2023, pp. 573–578. DOI: 10.1109/ICIDeA59866.2023.10295239.

[17] S. Reno, M. Ahmed, S. A. Jui, and S. Dilshad. "Securing Certificate Management System Using Hyperledger Based Private Blockchain". In: *2022 International Conference on Innovations in Science, Engineering and Technology (ICISET)*. Chittagong, Bangladesh, 2022, pp. 46–51. DOI: 10.1109/ICISET54810.2022.9775834.

[18] Manoj R and Sandeep Joshi. "Securing academic certificate verification with blockchain-based algorithmic rules". In: *2023 IEEE 4th International Multidisciplinary Conference on Engineering Technology (IMCET)*. 2023, pp. 242–247. DOI: 10.1109/IMCET59736.2023.10368253.

[19] R. R. Chandan, M. Lourens, K. K. Ramachandran, S. V. Akram, R. Bansal, and D. Kapila. "Implementation and Execution of Blockchain Technology in the Field of Education". In: *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*. Uttar Pradesh, India, 2022, pp. 1480–1485. DOI: 10.1109/IC3I56241.2022.10072593.

[20] Anjali Singh, SPS Chauhan, and Amit Kumar Goel. "Blockchain Based Verification of Educational and Professional Certificates". In: *2023 2nd International Conference on Computational Systems and Communication (ICCSC)*. 2023, pp. 1–7. DOI: 10.1109/ICCSC56913.2023.10143008.

[21] Mega Adi Kusuma, Parman Sukarno, and Aulia Arif Wardana. "Security System for Digital Land Certificate Based on Blockchain and QR Code Validation in Indonesia". In: *2022 International Conference on Advanced Creative Networks and Intelligent Systems (ICACNIS)*. 2022, pp. 1–6. DOI: 10.1109/ICACNIS57039.2022.10055114.

[22] Arunangshu Mojumder Raatul, Tasfia Rahman, Sumaiya Islam Mouno, and Nafees Mansoor. "RMT: A Lightweight Encryption Algorithm For Blockchain-Based Certificate Verification". In: *2023 IEEE 9th International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)*. 2023, pp. 232–236. DOI: 10.1109/WIECON-ECE60392.2023.10456497.

[23] Lei Xu, Xue Song, Jipeng Hou, and Liehuang Zhu. "Blockchain-based Certificate Management with Multi-Party Authentication". In: *2023 6th International Conference on Information and Computer Technologies (ICICT)*. 2023, pp. 211–219. DOI: 10.1109/ICICT58900.2023.00042.

[24] David Khoury, Patrick Balian, and Elie Kfoury. "Implementation of Blockchain Domain Control Verification (B-DCV)". In: *2022 45th International Conference on Telecommunications and Signal Processing (TSP)*. 2022, pp. 17–22. DOI: 10.1109/TSP55681.2022.9851252.

[25] Sumaiya Islam Mouno, Tasfia Rahman, Arunangshu Mojumder Raatul, and Nafees Mansoor. "Certiblock: The Exemplary Utilization of Blockchain for the Rigorous Validation of Academic Certificates". In: *2023 26th International Conference on Computer and Information Technology (ICCIT)*. 2023, pp. 1–6. DOI: 10.1109/ICCIT60459.2023.10441100.

[26] Avni Rustemi, Vladimir Atanasovski, and Aleksandar Risteski. "Identification During Verification Of Diplomas In The Blockchain System". In: *2023 30th International Conference on Systems, Signals and Image Processing (IWSSIP)*. 2023, pp. 1–5. DOI: 10.1109/IWSSIP58668.2023.10180241.

[27] Atik Zakirhusen Mujawar, Akash Lalitkumar Makwana, Lalit Shailesh Jain, Dev Vikesh Doshi, Smita Bansod, and Nivedeeta Mukherjee. "Blockchain qualified: Verification system". In: *2023 International Conference on Advanced Computing Technologies and Applications (ICACTA)*. 2023, pp. 1–6. DOI: 10.1109/ICACTA58201.2023.10393834.

[28] Jingnan Dong, Guangxia Xu, Chuang Ma, Jun Liu, and Uchani Gutierrez Omar Cliff. "Blockchain-Based Certificate-Free Cross-Domain Authentication Mechanism for Industrial Internet". In: *IEEE Internet of Things Journal* 11.2 (2024), pp. 3316–3330. DOI: 10.1109/JIOT.2023.3296506.

[29] Atta ur Rehman Khan and Raja Wasim Ahmad. "Blockchain-based Academic Degrees Issuance and Attestation". In: *2022 International Conference on IT and Industrial Technologies (ICIT)*. 2022, pp. 1–6. DOI: 10.1109/ICIT56493.2022.9989203.

[30] Xiao Tian, He Li, Qinglei Qi, Xiaofeng Xu, Rui Zhang, Huimei Jia, and Tianyang Liu. "Certificateless Aggregate Signature Authentication Scheme based on Blockchain in Smart Home Network". In: *2022 International Conference on 6G Communications and IoT Technologies (6GIoTT)*. 2022, pp. 49–53. DOI: 10.1109/6GIoTT57212.2022.00017.

Enhancing Trust and Integrity in Educational Certification Systems with Blockchain Credentials

Rakesh Modi
Computer Science and Engineering
Vardhaman College Of Engineering
Hyderabad, India
modir810@gmail.com

Nikhil Badam
Computer Science and Engineering
Vardhaman College Of Engineering
Hyderabad, India
nikhilb1608@gmail.com

Sayyed Shoheb
Computer Science and Engineering
Vardhaman College Of Engineering
Hyderabad, India
sayyedshohebsayyed123@gmail.com

Rayeesa Tasneem
Computer Science and Engineering
Vardhaman College Of Engineering
Hyderabad, India
rayeesa.tasneem3@gmail.com

***Abstract*—Blockchain technology has emerged as a powerful tool for securing and validating digital transactions across diverse industries, including education. In response to the rising concerns surrounding fraudulent certificates and their detrimental impact on trust and credibility, this paper introduces a comprehensive blockchain-based system specifically tailored for the issuance and verification of educational certificates.By harnessing the capabilities of Ethereum for smart contract functionality, IPFS for decentralized storage, Flask for web application development, and Truffle for smart contract deployment and testing, our system addresses the pressing need for a secure and reliable certification process. While fraudulent certificates pose a significant threat to the integrity of educational qualifications, our system offers a solution that mitigates this risk through robust authentication mechanisms and transparent verification processes. Unlike traditional paper-based or centralized digital certificates, our blockchain-based system ensures the immutability and tamper-proof nature of educational credentials. By streamlining the entire certification lifecycle—from university registration to certificate sharing among students, employers, and educational institutions—we provide stakeholders with a trusted platform to validate the authenticity of certificates. Moreover, our focus on educational certificates is driven by the increasing prevalence of fraudulent practices in the hiring process. With the proliferation of false credentials used by job applicants to secure employment, companies face significant challenges in verifying the qualifications of potential hires. By prioritizing the verification of educational certificates, our system aims to restore trust in the recruitment process and safeguard the integrity of professional qualifications.**

Keywords*—Decentralized process, Document verification, Blockchain, Ethereum, Smart contracts, Hashing, IPFS.

I. INTRODUCTION

The origins of Blockchain technology trace back to research scientists Stuart Haber and W. Scott Stornetta, although its widespread recognition surged in 2009 with the emergence of Bitcoin by Satoshi Nakamoto. Within the educational sector, Blockchain technology finds extensive applications, including the issuance and verification of documents (e-transcripts), cost-effective storage of large files, automated learning platforms, and mechanisms for publishing and copyright protection, as well as facilitating payments via cryptocurrencies [1]. Traditional methods of issuing paper degrees and certificates, followed by manual verification processes, are plagued by inefficiencies, necessitating extensive paperwork, emails, and phone calls, resulting in a slow and cumbersome process. This conventional system is riddled with issues such as certificate loss or damage, necessitating re-issuance, thereby compounding the problem. Additionally, the prevalence of document forgery undermines the integrity of credentials, leading to the employment of unqualified individuals, which can cost companies an average of $15,000 [2]. Studies indicate that over 30% of claimed degrees are falsified [3, 4]. Notably, in 2009, a court clerk faced legal action for fabricating documents to secure employment [5]. At MIT, Dean of Admissions Marilee Jones resigned after it was discovered she had misrepresented her qualifications from a New York university for nearly three decades [6]. Such incidents highlight the need for digitally verifiable credentials. Research by Ezell and Bear underscores the lucrative nature of the billion-dollar industry fueling these deceptive practices [7].

The objective of this paper is to propose a solution to the challenges associated with traditional paper-based educational certificates by leveraging blockchain technology, specifically on the Ethereum platform. The aim is to enhance efficiency in the verification process, reduce the risk of document loss or damage, and mitigate forgery through the creation of secure and easily verifiable digital certificates.

Traditional paper-based educational certificates pose challenges such as susceptibility to damage or loss, time-consuming manual verification processes, and vulnerability to forgery, leading to educational scams. This paper addresses these issues by proposing a blockchain-based

2020050314

ORIGINALITY REPORT

18%	11%	7%	13%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to VNR Vignana Jyothi Institute of Engineering and Technology Student Paper	4%
2	Submitted to Cerritos College Student Paper	3%
3	Submitted to Southern University And A & M College Student Paper	2%
4	Anjali Singh, SPS Chauhan, Amit Kumar Goel. "Blockchain Based Verification of Educational and Professional Certificates", 2023 2nd International Conference on Computational Systems and Communication (ICCSC), 2023 Publication	1%
5	Omar S. Saleh, Osman Ghazali, Norbik Bashah Idris. "A New Privacy-Preserving Protocol for Academic Certificates on Hyperledger Fabric", International Journal of Advanced Computer Science and Applications, 2023 Publication	1%

6	Submitted to UNITEC Institute of Technology Student Paper	1 %
7	5dok.org Internet Source	1 %
8	fastercapital.com Internet Source	1 %
9	Mohamed Ben Farah, Yussuf Ahmed, Haithem Mahmoud, Syed Attique Shah et al. "A survey on blockchain technology in the maritime industry: Challenges and future perspectives", Future Generation Computer Systems, 2024 Publication	<1 %
10	Lakshmana Kumar Ramasamy, Firoz Khan. "Chapter 5 Cross-Border Credit Transfer: Unlocking Educational Opportunities with Blockchain", Springer Science and Business Media LLC, 2024 Publication	<1 %
11	Submitted to Jawaharlal Nehru Technological University Student Paper	<1 %
12	"Proceedings of Second International Conference on Intelligent System", Springer Science and Business Media LLC, 2024 Publication	<1 %

13	Shiva Chaithanya Goud Bollipelly, Prabu Sevugan, R. Venkatesan, L. Sharmila. "chapter 21 Blockchain-Based Messaging System for Secure and Private Communication", IGI Global, 2023 Publication	<1%
14	R. Elakya, R. Thanga Selvi, T. Manoranjitham, S. Shanthana. "chapter 10 Synergizing AI and Blockchain", IGI Global, 2024 Publication	<1%
15	insights2techinfo.com Internet Source	<1%
16	C Madanagopal, Ms Kaniskaa. "Blockchain based Letter of Recommendation Verification System for Higher Studies", 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), 2023 Publication	<1%
17	Submitted to Edith Cowan University Student Paper	<1%
18	www.coursehero.com Internet Source	<1%
19	www.tdx.cat Internet Source	<1%
20	www.springboard.com Internet Source	<1%

21	Submitted to ESC Rennes Student Paper	<1%
22	Submitted to Institute of Research & Postgraduate Studies, Universiti Kuala Lumpur Student Paper	<1%
23	Submitted to The University of the West of Scotland Student Paper	<1%
24	Submitted to Gitam University Student Paper	<1%
25	Submitted to Luton Sixth Form College, Bedfordshire Student Paper	<1%
26	Submitted to University of New Haven Student Paper	<1%
27	www.geoparquearouca.com Internet Source	<1%
28	Submitted to Wawasan Open University Student Paper	<1%
29	www.lightflows.co.uk Internet Source	<1%
30	Submitted to Indian Institute of Information Technology, Design and Manufacturing - Kancheepuram Student Paper	<1%

31	Daniel Chiș, Mihai Caramihai. "Blockchain in Higher Education: A Secure Traceability Architecture for Degree Verification.", IntechOpen, 2023 Publication	<1 %
32	www.i2home.org Internet Source	<1 %
33	Rafah Amer Jaafar, Saad Najim Alsaad. "Enhancing Educational Certificate Verification With Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric", TEM Journal, 2023 Publication	<1 %
34	davcollegetitilagarh.org Internet Source	<1 %
35	gecgudlavalleru.ac.in Internet Source	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		