BCL PROJECT REPORT

on

Certification Validation System

By

120A3036 Subodh Patil

120A3040 Ankur Rai

120A3042 Ruchir Rao

120A3044 Shubham Sankpal

UNDER THE GUIDANCE OF

Prof. Poornima

SUBMITTED IN PARTIAL FULFILLMENT FOR THE DEGREE OF

BACHELOR OF ENGINEERING

In Information Technology

DEPARTMENT OF INFORMATION TECHNOLOGY

SIES GRADUATE SCHOOL OF TECHNOLOGY

NERUL, NAVI MUMBAI – 400706

ACADEMIC YEAR

2023-2024

CERTIFICATE

This is to certify that this is a bonafide record of BCL Project of the project titled **"Certificate Validation System"**

carried out by the following students of Fourth year in Information Technology.

Sr. No.	Name	Roll No.
1.	Subodh Patil	120A3036
2.	Ankur Rai	120A3040
3.	Ruchir Rao	120A3042
4.	Shubham Sankpal	120A3044

The report is submitted in partial fulfillment of the degree course of Bachelor of Engineering in Information Technology, of University of Mumbai during the academic year 2023-24

Internal Guide	**Head of Department**	**Principal**
Prof. Poornima	Mrs. Seema Redekar	Dr. Lakshmi Sudha

We have examined this report as per University requirements at SIES Graduate School of Technology, Nerul (E), Navi Mumbai on_____.

Name of External Examiner:

Signature with Date:

Name of Internal Examiner:

Signature with Date:

ACKNOWLEDGEMENT

We wish to express our deep sense of gratitude to thank our project guide Prof. Poornima for providing timely assistance to our query and guidance. We take this opportunity to thank our HOD Mrs. Seema Redekar and Principal Dr. Lakshmi Sudha for their valuable guidance and immense support in providing all the necessary facilities.

We would also like to thank the entire faculty of the IT Department for their valuable ideas and timely assistance in this project. Last but not the least, we would also like to thank teaching and nonteaching staff members of our college for their support, in facilitating timely completion of the mini project.

Project Team

Subodh Patil	120A3036
Ankur Rai	120A3040
Ruchir Rao	120A3042
Shubham Sankpal	120A3044

CONTENTS

ABSTRACT

In today's digital age, the verification of certificates and credentials is critical across various domains, including education, employment, and professional certifications. However, traditional methods of certificate validation often face challenges such as fraud, tampering, and inefficiency. To address these issues, this paper proposes a novel Certificate Validation System (CVS) utilizing blockchain technology.

The proposed system leverages the inherent properties of blockchain, including immutability, decentralization, and transparency, to establish a trustworthy and tamper-proof mechanism for verifying certificates. Each certificate is cryptographically hashed and stored as a transaction on the blockchain network, ensuring its integrity and preventing unauthorized alterations.

The validation process involves querying the blockchain for the presence of the certificate hash, enabling instant and secure verification of its authenticity. Moreover, the decentralized nature of the blockchain eliminates the reliance on a central authority, reducing the risk of single points of failure and enhancing trust among stakeholders.

Furthermore, smart contracts are employed to automate and enforce validation rules, facilitating seamless interactions between certificate issuers, recipients, and verifiers. Through the use of smart contracts, the system can implement customized validation criteria, such as expiration dates, accreditation requirements, and revocation mechanisms, enhancing flexibility and adaptability.

In addition to enhancing security and efficiency, the proposed CVS offers several benefits, including increased transparency, reduced administrative overhead, and improved interoperability across disparate systems. Moreover, by leveraging blockchain technology, the system ensures data privacy and confidentiality, safeguarding sensitive information from unauthorized access.

Overall, the Certificate Validation System presented in this paper represents a significant advancement in ensuring the authenticity and integrity of certificates in a digital environment. By harnessing the power of blockchain, the system provides a robust and reliable solution to the challenges associated with traditional certificate validation methods, ultimately fostering trust and credibility in credential verification processes.

Chapter 1
Problem Statement

In contemporary society, the verification of certificates and credentials is a pivotal process across various sectors such as education, employment, and professional certifications. However, conventional methods of certificate validation are plagued by several challenges that compromise their integrity, authenticity, and efficiency.

Fraudulent Activities: Traditional paper-based certificates are susceptible to forgery and manipulation, leading to an increase in fraudulent activities such as the production of counterfeit degrees or credentials.

Centralized Validation Authorities: Existing validation systems often rely on centralized authorities to verify certificates, resulting in a single point of failure and potential vulnerabilities to hacking, data breaches, or manipulation by malicious actors.

Cost and Time-Intensive Processes: The manual verification of certificates can be time-consuming, resource-intensive, and prone to errors, particularly when dealing with a large volume of documents or across international borders.

Lack of Transparency: In many cases, the validation process lacks transparency, making it challenging for stakeholders to verify the authenticity and legitimacy of certificates, leading to a loss of trust and credibility in the validation process.

Limited Interoperability: Existing validation systems often lack interoperability between different organizations, platforms, or jurisdictions, hindering the seamless exchange and recognition of credentials across borders or industries.

Addressing these challenges requires a paradigm shift towards a more secure, transparent, and efficient certificate validation system. Leveraging blockchain technology presents a promising solution by providing a decentralized, immutable, and transparent ledger to store and validate certificate data. By decentralizing the validation process and ensuring data integrity through cryptographic techniques, a blockchain-based Certificate Validation System (CVS) can overcome the limitations of traditional methods and establish a trusted and tamper-proof mechanism for verifying certificates.

1.1 Objective

The primary objective of the Certificate Validation System (CVS) utilizing blockchain technology is to establish a secure, transparent, and efficient mechanism for verifying the authenticity and integrity of certificates and credentials. Specifically, the objectives include:

Transparency and Trust: Leveraging the transparency and immutability of the blockchain to provide stakeholders with visibility into the entire lifecycle of certificates, including issuance, validation, and revocation, fostering trust and confidence in the validation process.

Interoperability: Facilitating seamless exchange and recognition of certificates across different organizations, platforms, and jurisdictions by standardizing validation protocols and leveraging the interoperability features of blockchain networks, thereby enhancing the portability and accessibility of credentials.

Data Privacy and Confidentiality: Ensuring the privacy and confidentiality of sensitive certificate data by implementing privacy-enhancing techniques such as zero-knowledge proofs or encrypted data storage on the blockchain, thereby protecting the personal information of certificate holders while still enabling verification.

Compliance and Regulation: Enabling compliance with regulatory requirements and accreditation standards by implementing customizable validation rules and protocols within smart contracts, ensuring adherence to industry-specific regulations and standards.

By achieving these objectives, the Certificate Validation System using blockchain technology aims to revolutionize the process of certificate verification, overcoming the limitations of traditional methods and providing a trusted, efficient, and scalable solution for verifying credentials across various domains and industries.

1.2 Literature Survey

Sr. No.	Author	Title	Key Findings/ Gap
1	Avni Rustemi, Fisnik Dalipi, Vladimir Atanasovski, Aleksandar Risteski	A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification	This paper presents the importance of Building a secure Certificate Validation System that offers the integrity and privacy of Certificate Ownership.
2	Semi Yulianto, Harco Leslie Hendric Spits Warnars, Harjanto Prabowo	Security Risks and Best Practices for Blockchain and Smart Contracts: A Systematic Literature Review	This paper shows how to create secure smart contracts for a blockchain network to implement this is Certificate Validation System.
3	Satpal Singh Kushwaha, Sandeep Joshi, Dilbag Singh, Manjit Kaur, Heung-No Lee	Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract	This paper reviews the security vulnerabilities in Ethereum Blockchain.
4	Syada Tasmia Alvi, Mohammed Nasir Uddin,Linta Islam, Sajib Ahamed	Security Evaluation of Smart Contracts based on Code and Transaction - A Survey	This paper Concentrates on a systematic analysis of multiple forms of voting with blockchain and without blockchain by numerous researchers
5	Jianzhong Su, Jiyi Liu, Yuhong Nan, Yin Li	Security Evaluation of Smart Contracts based on Code and Transaction - A Survey	Blockchain, Smart contract , Ethereum, Security

Chapter 2
Proposed System

2.1 Introduction

In an increasingly digital world, the verification of certificates and credentials is vital across numerous sectors. Yet, traditional methods often grapple with issues like fraud and inefficiency. To mitigate these challenges, we present a groundbreaking solution: a Certificate Validation System (CVS) employing blockchain technology. By leveraging blockchain's immutable and transparent ledger, the CVS aims to revolutionize the verification process, ensuring certificates remain tamper-proof and authentic.

Blockchain serves as the backbone of the proposed CVS, offering unparalleled security and transparency. Each certificate is hashed and stored on the blockchain, creating an indelible record of its validity. This decentralized approach removes the reliance on a central authority, reducing the risk of fraud and manipulation. Through automated validation and smart contracts, the system streamlines the verification process, saving time and resources while enhancing trust and reliability.

With the CVS, we aim to address the shortcomings of traditional certificate validation methods. By harnessing blockchain's transformative capabilities, we pave the way for a more secure, efficient, and transparent credential verification process. From education to employment, the CVS offers a robust solution to ensure the integrity and authenticity of certificates in the digital age.

2.2 Details of Hardware and Software Requirements

Hardware:

Processor: Intel i3 or higher

RAM : 4GB or higher

ROM : 128GB minimum

Internet Connection

Software:

VS Code: Code Editor for writing code

Ganache-cli: For local blockchain network

Truffle: For smart contract development and deployment

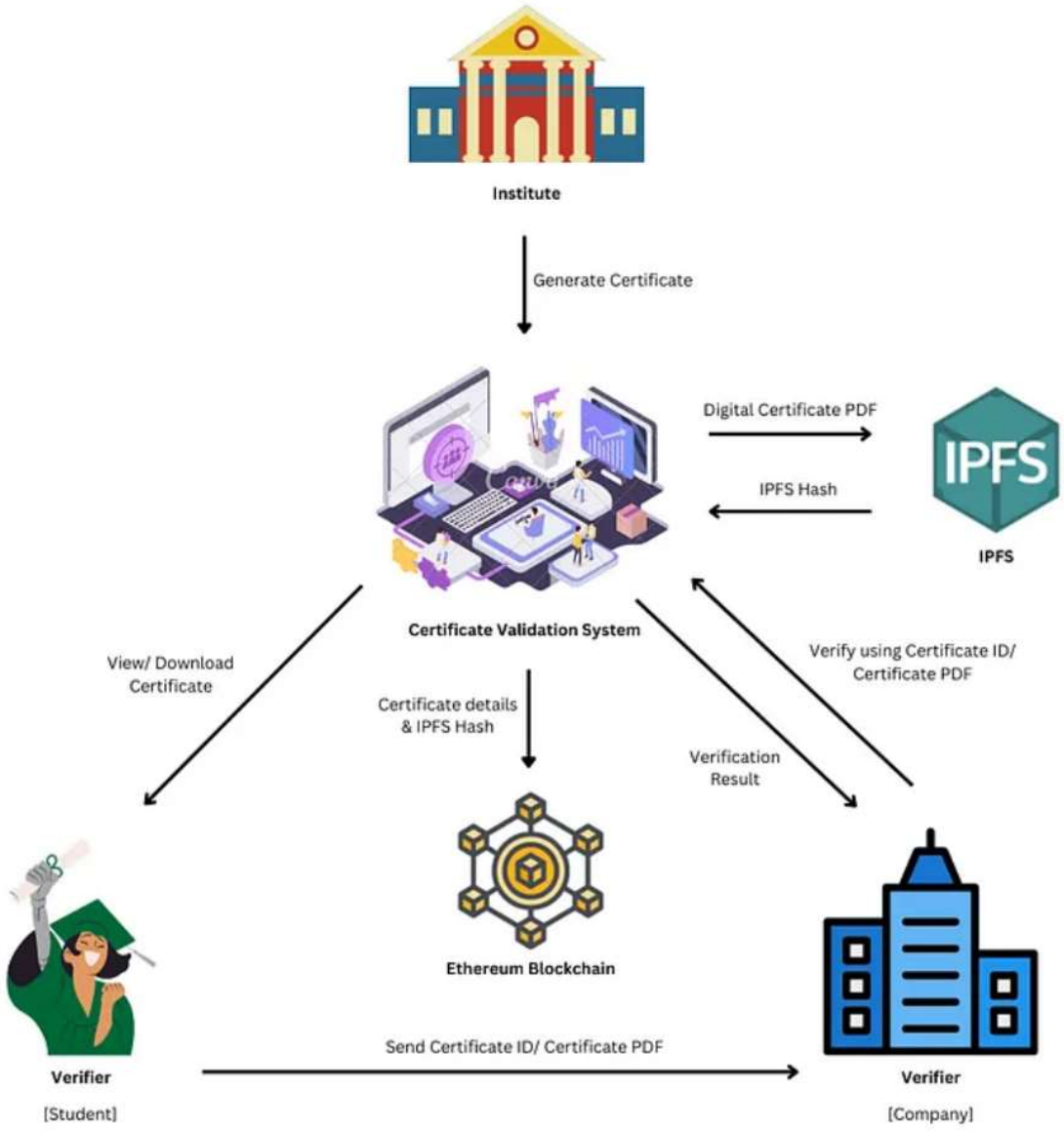
Solidity : Programming Language for implementing smart contract

Streamlit (Python Web Framework) : For developing the web application

Pinata: An IPFS client to store validated certificates

Firebase Authentication : To Authenticate users , using the System.

2.3 System Architecture



The system comprises of 2 main entities:

Institute: Responsible for generating and issuing certificates. Has the functionality to generate and view certificates.

Verifier: Responsible for verifying certificates. Has the functionality to verify certificates by either uploading a certificate pdf or by inputting the certificate id.

Chapter 3

Implementation

3.1 Code

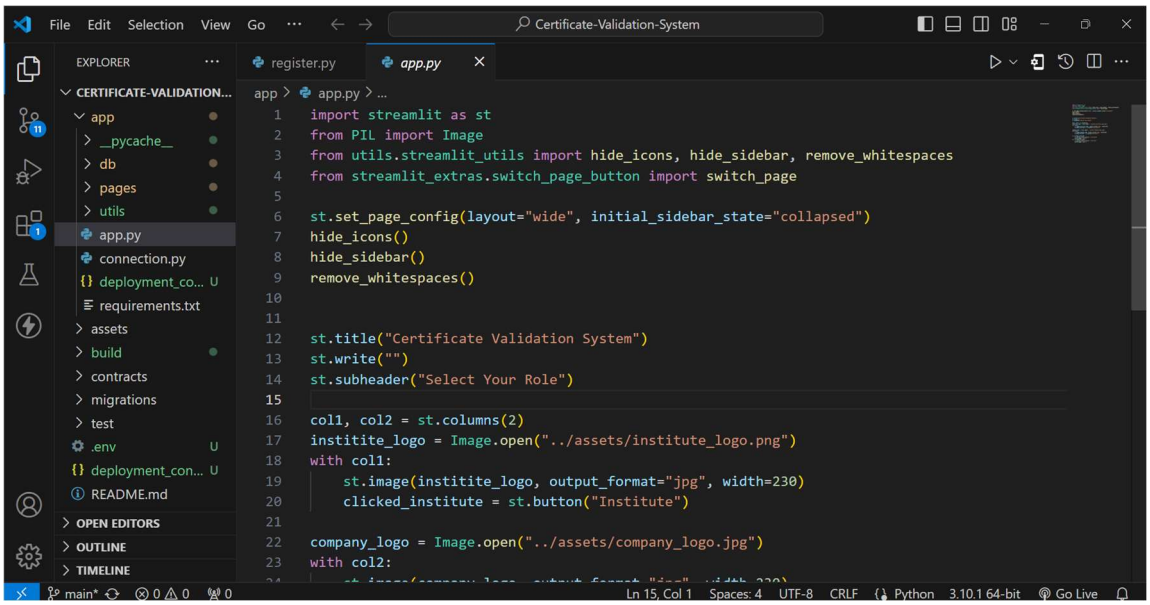


Fig 3.1.1 : app.py

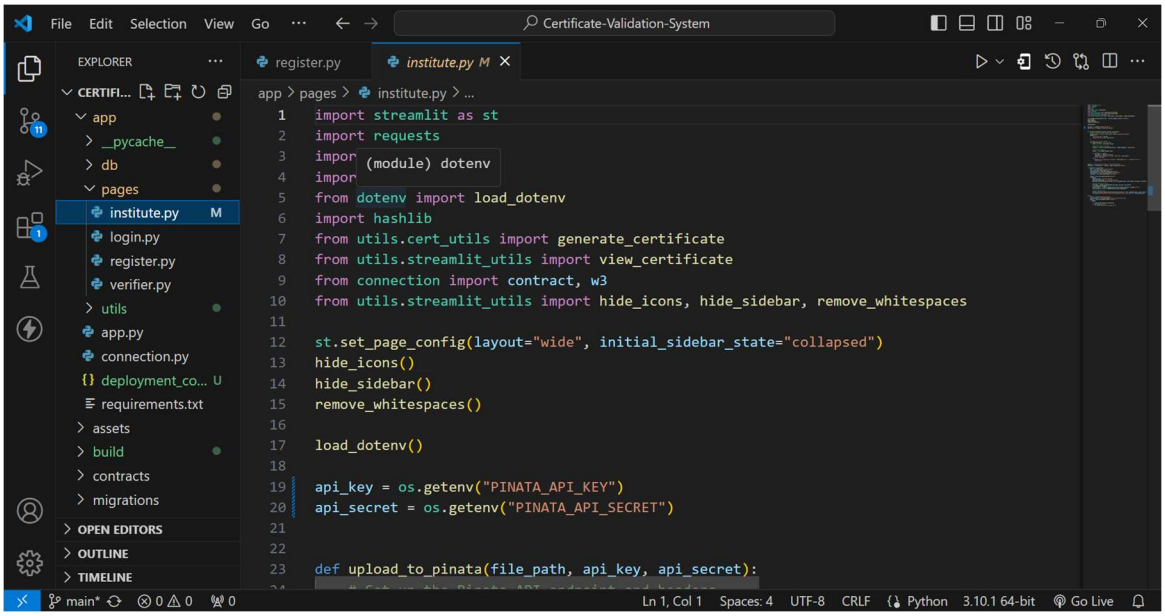


Fig 3.1.2 : institute.py

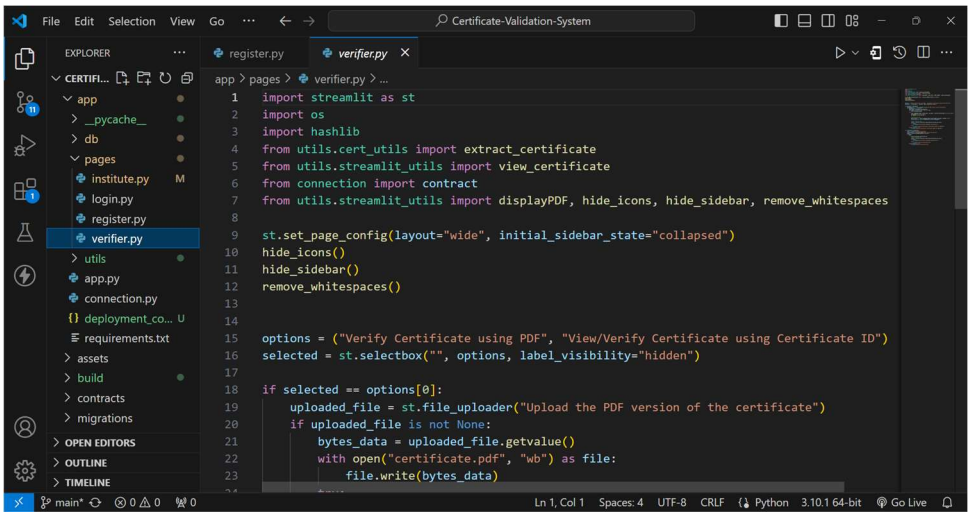


Fig 3.1.3 : verifier.py

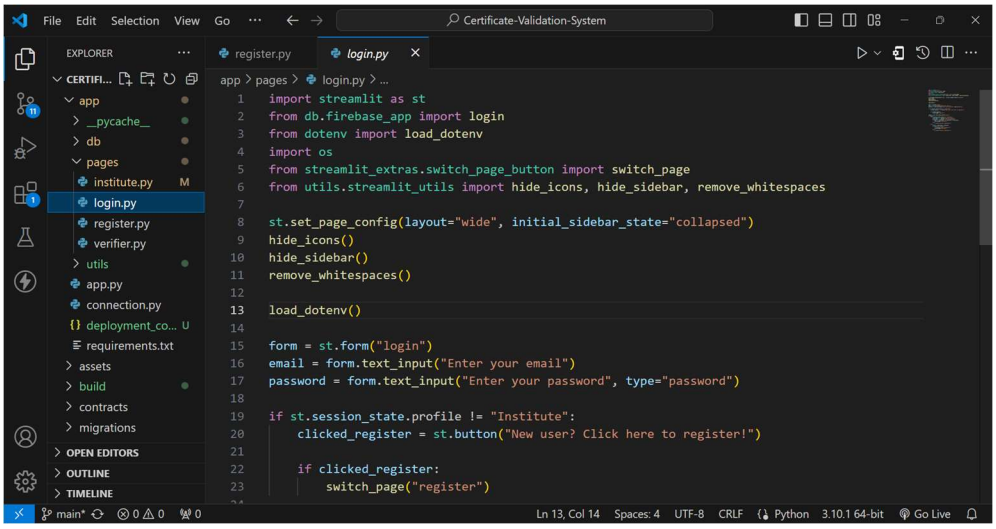


Fig 3.1.4 : login.py

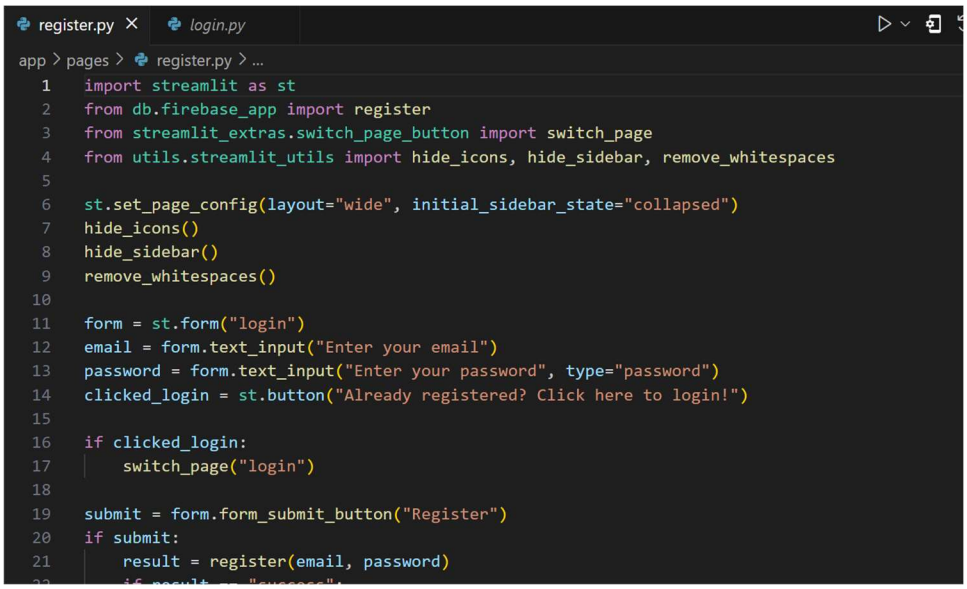


Fig 3.1.5 : register.py

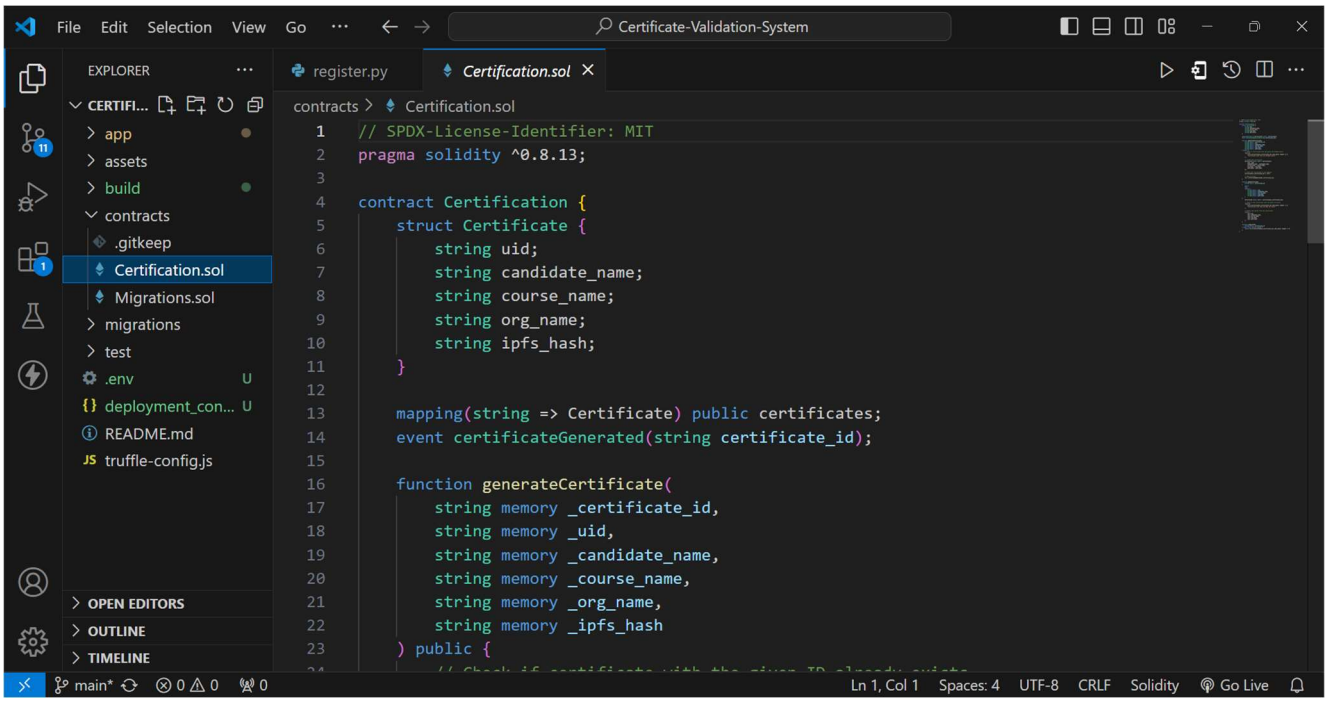


Fig 3.1.6: Certification.sol

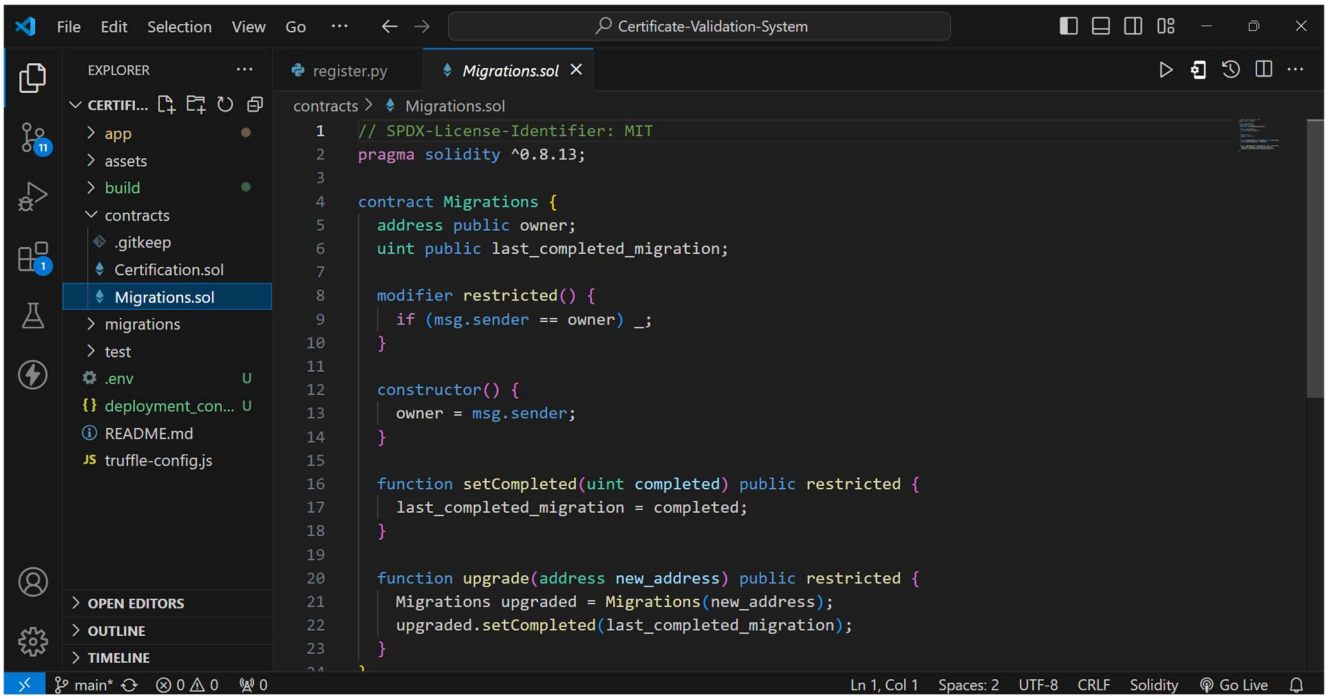


Fig 3.1.7: Migrations.sol

3.2 Experimental Results

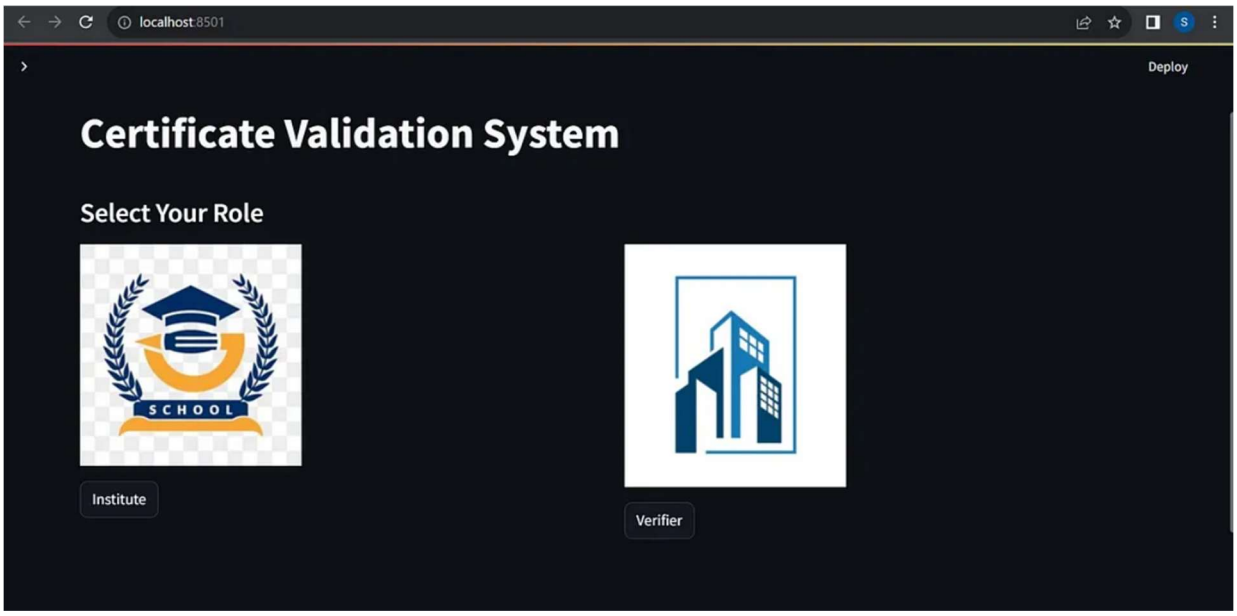


Fig 3.2.1: Home Page

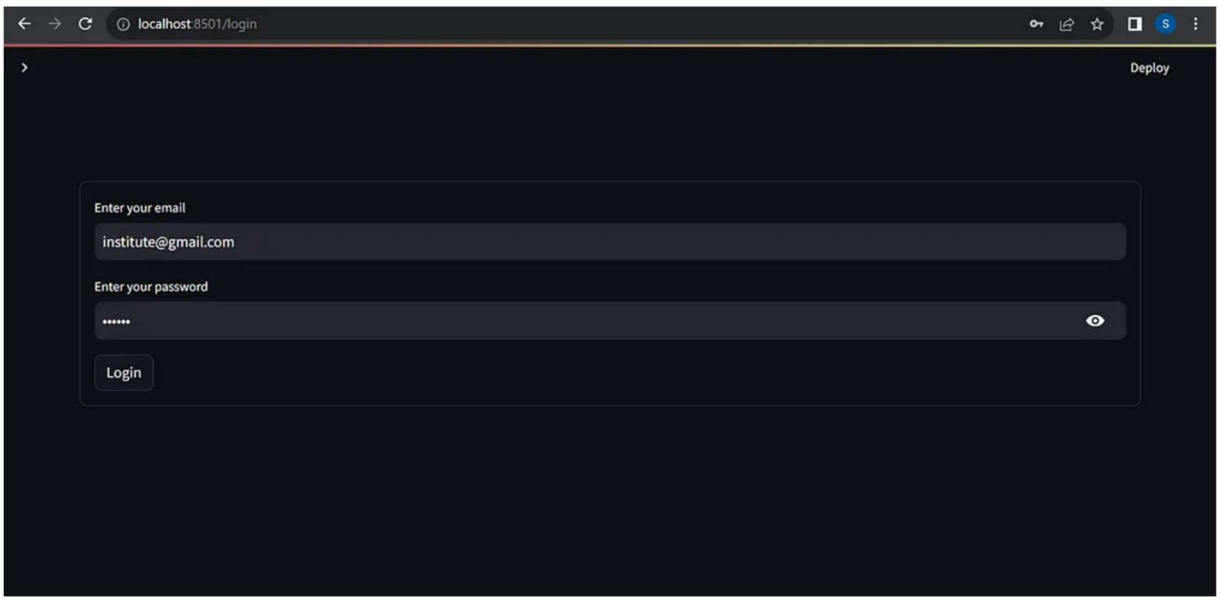


Fig 3.2.2: Login Page

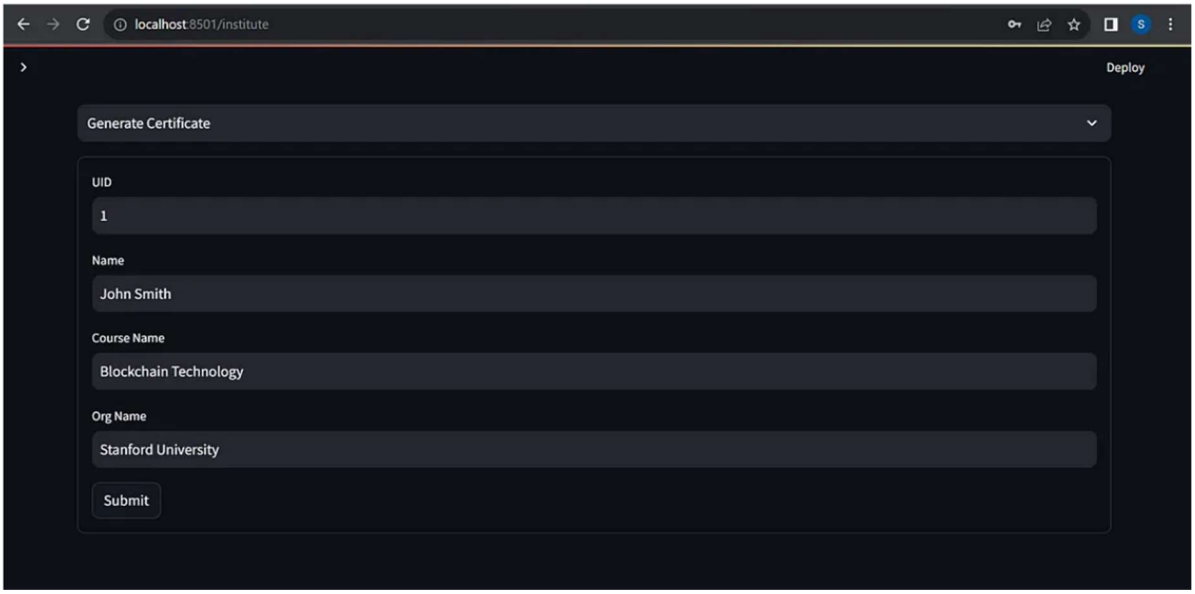


Fig 3.2.3: Generate Certificate

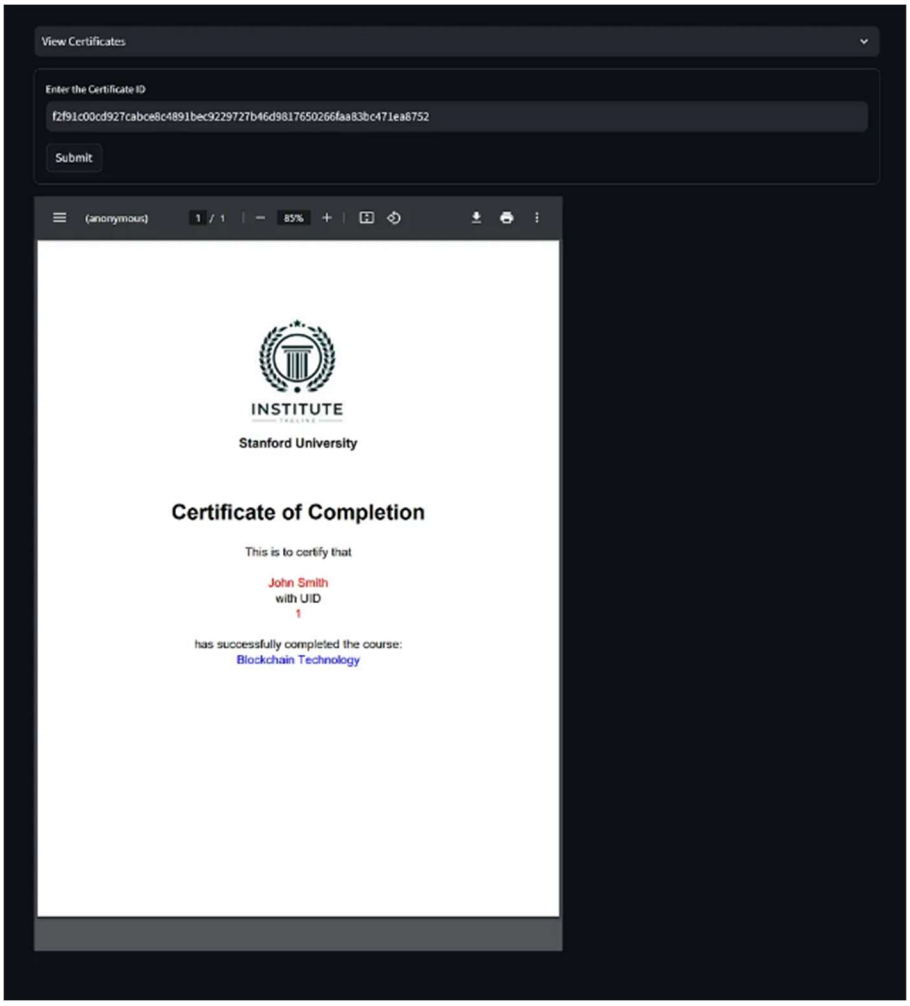


Fig 3.2.4: Validation Page

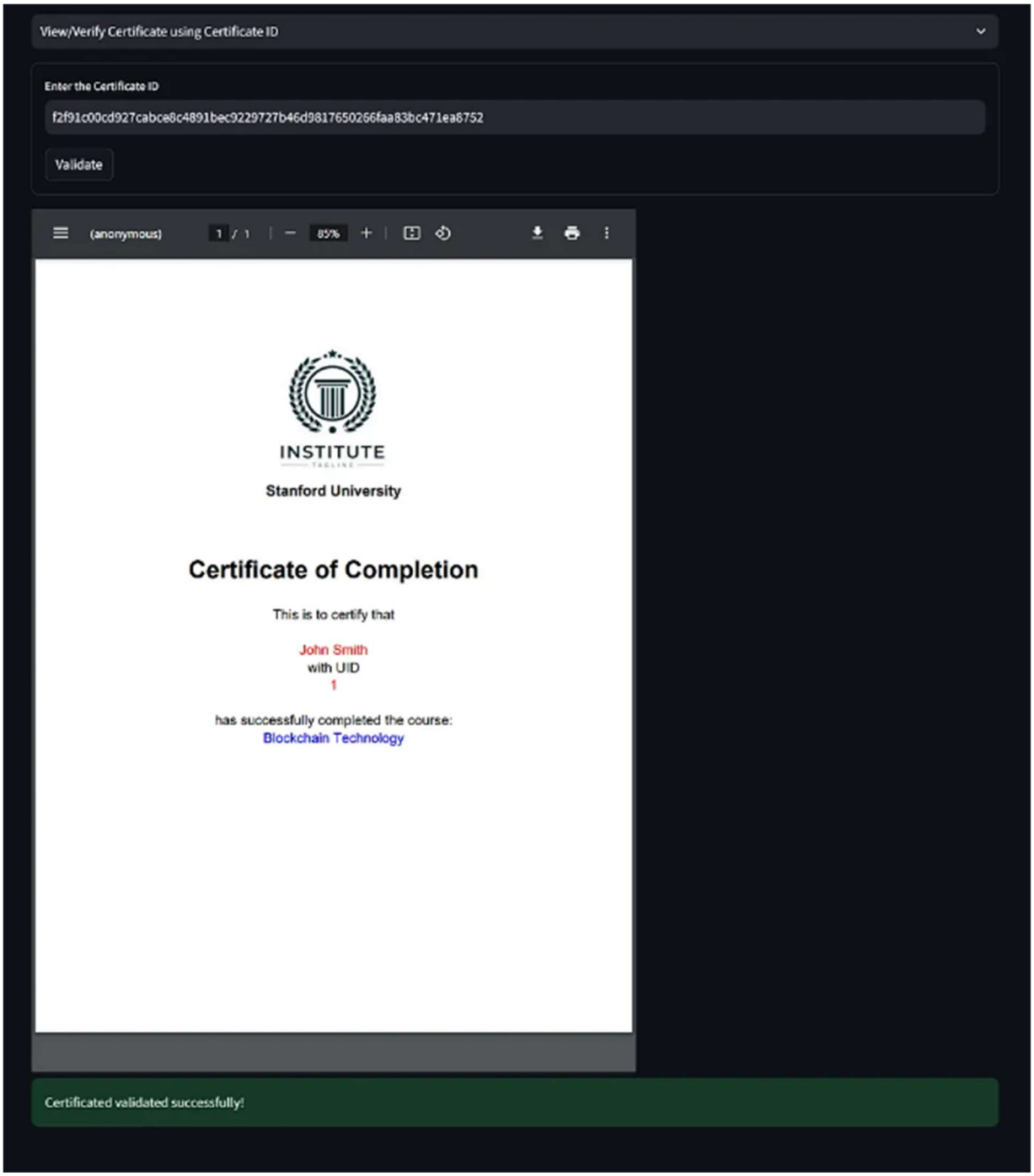


Fig 3.2.5: Validation using Certificate ID

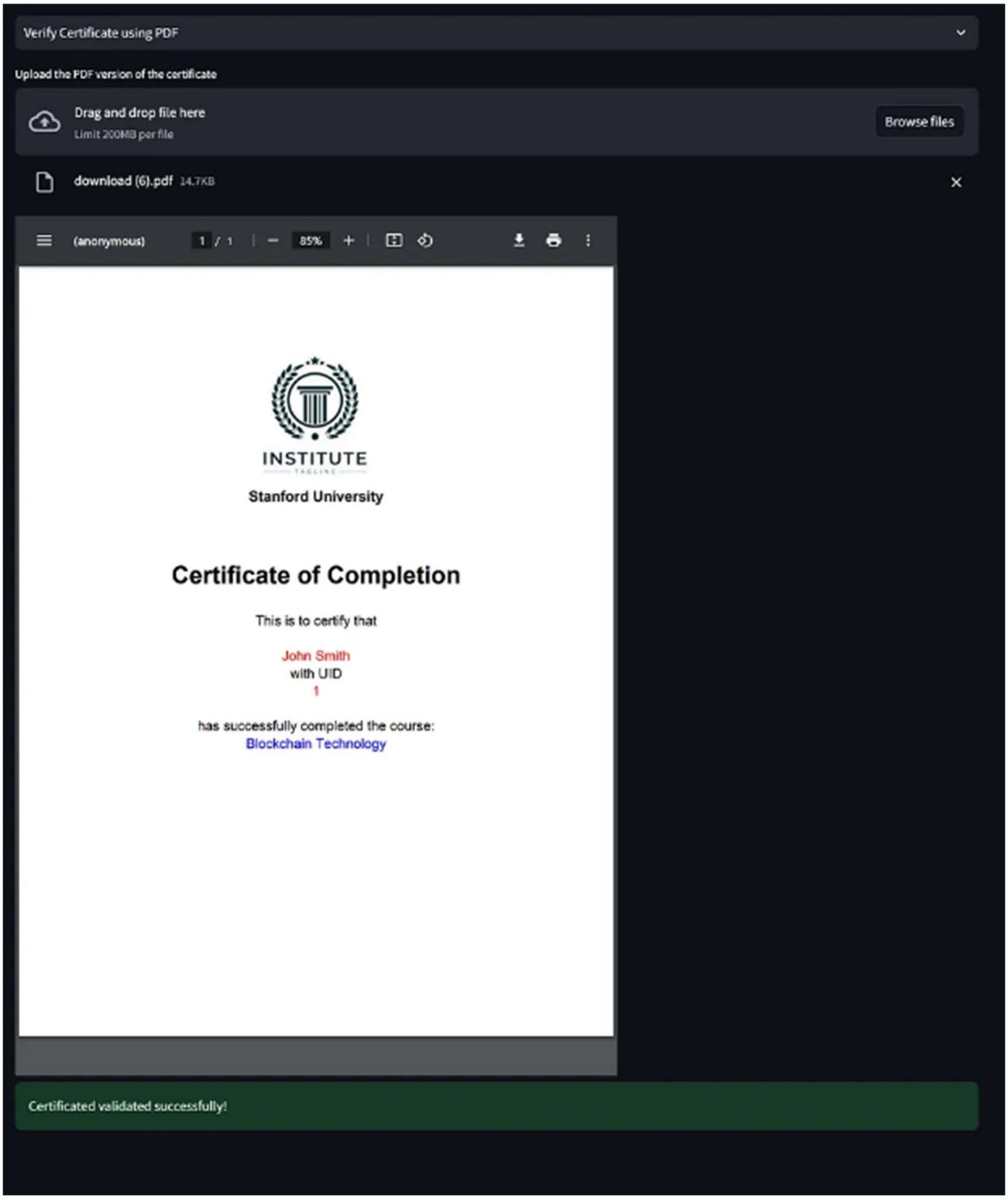


Fig 3.2.6: Validation using Certificate PDF

Chapter 4
Contribution

4.1 Result

The implementation of the Certificate Validation System (CVS) utilizing blockchain technology has yielded transformative outcomes, marking a significant advancement in certificate verification processes.

Firstly, the system has significantly enhanced the security of certificate validation by leveraging blockchain's immutable ledger and cryptographic mechanisms. Certificates are stored as hashed transactions on the blockchain, ensuring their integrity and authenticity. This tamper-proof nature of blockchain has effectively mitigated the risk of fraudulent activities, bolstering trust and confidence in the validation process.

Secondly, the CVS has led to substantial improvements in efficiency by automating validation tasks and reducing manual intervention. With the deployment of smart contracts, verification processes are executed seamlessly, resulting in faster turnaround times for certificate validation. This streamlined approach has not only saved valuable time but also optimized resource allocation within organizations.

Thirdly, blockchain's transparent ledger has facilitated unparalleled visibility into the lifecycle of certificates, enhancing transparency and accountability. Stakeholders can access real-time, verifiable information about certificates, reducing the likelihood of disputes or discrepancies. This transparency fosters trust among stakeholders and ensures the integrity of the validation process.

Lastly, the CVS has enabled cost reduction through automation and elimination of intermediaries. By minimizing operational costs associated with manual validation methods, organizations can allocate resources more efficiently. This cost-effectiveness not only improves the financial viability of certificate validation but also allows organizations to redirect savings towards strategic initiatives or enhancing service quality for stakeholders.

4.2 Conclusion

In conclusion, the implementation of the Certificate Validation System (CVS) using blockchain technology has brought about a profound transformation in certificate verification processes. By harnessing the power of blockchain's immutable ledger and cryptographic mechanisms, the CVS has effectively tackled longstanding challenges in the validation landscape, such as fraud, inefficiency, and lack of transparency.

The outcomes of the CVS deployment underscore its remarkable benefits across various dimensions. Through enhanced security measures, the system has ensured the integrity and authenticity of certificates, fostering trust and reliability among stakeholders. Additionally, the automation and transparency facilitated by the CVS have significantly improved efficiency, streamlining validation processes and reducing operational costs for organizations involved in certificate verification.

Overall, the CVS represents a pioneering step towards modernizing certificate validation in the digital age. By leveraging blockchain technology, the system has laid a robust foundation for a secure, efficient, and transparent framework for verifying certificates across diverse sectors. As digital credentials continue to evolve, the CVS stands as a testament to innovation, driving progress and instilling confidence in credential verification processes worldwide.

4.3 References

[1] [Rushby93] Rushby, John, "Formal Methods and the Certification of Critical Systems," *SRI-CSL Technical Report*, November 1993.

[2] [Kopetz97] Kopetz, Herman, *Real-Time Systems: Design Principles for Distributed Embedded Applications*, Boston, MA: Kluwer Academics Publishers, 1997.

[3] [NASA99] NASA Software Independent Verification & Validation Facility, http://www.ivv.nasa.gov, accessed May 5, 1999.

[4] [Andriole86] Andriole, Stephen J., editor, *Software Validation, Verification, Testing, and Documentation*, Princeton, NJ: Petrocelli Books, 1986.

[5] [RTCA92] RTCA-DO-178B, Software Considerations in Airborne Systems and Equipment Certification, December 1992.