Certificate Validation Using Blockchain Ethvalidify

A PROJECT REPORT

Submitted by,

Mr. Nandeesh Gowda C	**- 20201CSE0697**
Mr. Hruthik S	**- 20201CSE0682**
Mr. Sudarsh V	**- 20201CSE0683**

Under the guidance of,

Ms. Naiwrita Borah

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

At

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY

BENGALURU

JANUARY 2024

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the Project report **“Certificate Validation Using Blockchain-Ethvalidify”** being submitted by “NANDEESH GOWDA C, HRUTHIK S, SUDARSH V” bearing roll numbers “20201CSE0697, 20201CSE0682, 20201CSE0683” in partial fulfilment of requirement for the award of degree of Bachelor of Technology in COMPUTER SCIENCE AND ENGINEERING is a bonafide work carried out under my supervision.

Ms.Naiwrita Borah Assistant Professor School of CSE Presidency University	**Dr. Pallavi R** Associate Professor& HoD School of CSE Presidency University

Dr. C. KALAIARASAN Associate Dean School of CSE&IS Presidency University	**Dr.L. SHAKKEERA** Associate Dean School of CSE&IS Presidency University	**Dr. SAMEERUDDIN KHAN** Dean School of CSE&IS Presidency University

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

We hereby declare that the work, which is being presented in the project report entitled **Certificate Validation using Blockchain - Ethvalidify** in partial fulfillment for the award of Degree of **Bachelor of Technology** in **Computer Science and Engineering**, is a record of our own investigations carried under the guidance of supervisor **Ms. Naiwrita Borah, Assistant Professor, School of Computer Science and Engineering, Presidency University, Bengaluru.**

We have not submitted the matter presented in this report anywhere for the award of any other Degree.

NAME	ROLL NUMBER	SIGNATURE
Nandeesh Gowda C	20201CSE0697	
Hruthik S	20201CSE0682	
Sudarsh V	20201CSE0683	

ABSTRACT

In today's digital age, guaranteeing the credibility and legitimacy of certificates and credentials is paramount. Conventional methods of verifying certificates encounter issues surrounding security, trustworthiness, and accessibility. This initiative aims to tackle these obstacles by harnessing blockchain technology to establish a secure and unchangeable system for certifying credentials. The proposed system employs a decentralized blockchain network to securely store and manage certificates. Each certificate undergoes cryptographic hashing and is documented on the blockchain, forming an unalterable and transparent record. Smart contracts are utilized to automate the verification process, streamlining the validation of certificates without necessitating intermediaries. Users engage with the system through an intuitive interface, allowing them to submit certificates for validation of the legitimacy of the certificate. A convincingly crafted counterfeit certificate is challenging to distinguish from the genuine original. As instances of fraudulent documents rise, the credibility of both the individual holding the certificate and the issuing authority becomes compromised. The system promptly delivers dependable verification outcomes, guaranteeing the trustworthiness and integrity of presented credentials. We are creating a system in which an institute can upload student Credentials to a community blockchain network. Also to authenticate the institute we are introducing another actor named Central Authority which can add the new institutes to the network. At last, comes the employer who can verify the deployed Certificate. Furthermore, the decentralized nature of blockchain ensures transparency in the validation process, eradicating reliance on centralized authorities and mitigating the risk of counterfeit certificates. Additionally, we will be utilizing the meta mask crypto wallet for deploying the certificates and infura as our node for connecting with the Ethereum blockchain. In the paper discussed below, we tried our best to find out the answers to the loopholes in the certificate validation by utilizing an advanced technology called Blockchain.

ACKNOWLEDGEMENTS

First of all, we are indebted to the **GOD ALMIGHTY** for allowing me to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected dean **Dr. Md. Sameeruddin Khan**, Dean, School of Computer Science and Engineering, Presidency University for getting us permission to undergo the project.

We record our heartfelt gratitude to our beloved Associate Deans **Dr. Kalaiarasan C and Dr. Shakkeera L,** School of Computer Science and Engineering, Presidency University and Dr. Pallavi R, Head of the Department, School of Computer Science and Engineering, Presidency University for rendering timely help for the successful completion of this project.

We are greatly indebted to our guide **Ms. Naiwrita Borah,** Assistant Professor, School of Computer Science and Engineering, Presidency University for her inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the project work.

We would like to convey our gratitude and heartfelt thanks to the University Project-II Coordinators **Dr. Sanjeev P Kaulgud, Dr. Mrutyunjaya MS** and also the department Project Coordinators **Mr. Zia Ur Rahman, Mr. Peniel John Whistely** .

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

Nandeesh Gowda C	**- 20201CSE0697**
Hruthik S	**- 20201CSE0682**
Sudarsh V	**- 20201CSE0683**

LIST OF FIGURES

CONTENTS OF TABLE

CHAPTER-1

INTRODUCTION

Certificates serve as pivotal instruments across diverse sectors, attesting to educational achievements, professional competencies, and legal qualifications. However, the traditional methods of validating these certificates often encounter challenges such as fraud, inefficiencies, and a lack of a standardized verification system. The advent of blockchain technology introduces a transformative solution by offering a decentralized and tamper-resistant platform for the validation of certificates.

This report explores the application of blockchain for certificate validation, elucidating the potential advantages it brings to security, transparency, and efficiency in the verification process. As the demand for reliable and secure validation mechanisms grows, the integration of blockchain technology emerges as a promising solution to overcome the limitations of conventional approaches. This introduction sets the stage for a comprehensive examination of the benefits, challenges, case studies, and future trends associated with leveraging blockchain for certificate validation. Through this exploration, we aim to provide valuable insights into the transformative potential of blockchain in ensuring the integrity and reliability of certificates across various industries.

1.1Background

1.1.1 Overview of the importance of certificates in different domains.

Certificates play a pivotal role across various domains, serving as formalized documentation that verifies an individual's attainment of specific knowledge, skills, or qualifications. The importance of certificates extends across diverse sectors, and their significance can be elucidated within the following domains:

1. Education: In the education sector, certificates, such as diplomas and degrees, authenticate the successful completion of educational programs. They serve as tangible evidence of an individual's academic prowess and are essential for pursuing further studies or entering the workforce.

2. Industry Competence: Certificates are often awarded for the successful completion of professional training programs and certification exams. In fields like IT, healthcare,

finance, and project management, certifications validate an individual's specialized skills and competence, making them more marketable in their respective industries.

3. Employment: Certificates act as credentials that employers seek when assessing the qualifications of potential hires. Job-specific training certificates or vocational certifications demonstrate that an individual possesses the necessary skills and knowledge required for a particular role.

4. Legal and Compliance: Certificates are used in legal contexts to validate various documents such as birth certificates, marriage certificates, and property deeds. These certificates hold legal significance and are crucial for establishing identity, relationships, and ownership.

5. Business and Industry: Certificates, such as ISO certifications, signify that a business adheres to specific quality standards. These certificates enhance trust among clients, partners, and consumers, showcasing a commitment to quality and compliance within the industry.

6. Technology and Skills Development: Certificates are awarded for completing workshops, online courses, or skill development programs. These certificates are instrumental in showcasing an individual's commitment to continuous learning and staying updated in rapidly evolving fields.

In summary, certificates are fundamental instruments that validate achievements, qualifications, and competencies across a spectrum of domains. Their importance lies in providing tangible proof of an individual's capabilities, facilitating trust, and serving as gateways to opportunities in education, employment, and various professional endeavors.

1.1.2 Challenges associated with the traditional certificate validation method

Traditional certificate validation methods, while widely used, face several challenges that can compromise their effectiveness. These challenges often revolve around issues of security, efficiency, and adaptability. Here are some key challenges associated with traditional certificate validation methods:

1. Forgery and Fraud: Traditional certificates, especially paper-based ones, are susceptible to forgery and fraudulent activities. With advancements in technology, replicating or altering physical certificates has become easier, posing a significant risk to the integrity of the validation process.

2. Limited Accessibility: Physical certificates are often stored in disparate locations, making them challenging to access and verify in a timely manner. This limitation can hinder employers, educational institutions, or other stakeholders from quickly and efficiently confirming the authenticity of a certificate.

3. Risk of Damage or Loss: Physical certificates are vulnerable to damage, loss, or deterioration over time. Fires, floods, or other unforeseen events can destroy paper certificates, making it difficult or impossible to retrieve and validate important credentials.

4. Dependency on Centralized Authorities: Many traditional validation methods rely on centralized authorities or institutions to confirm the legitimacy of certificates. This dependence can lead to delays in the validation process and raises concerns about single points of failure or corruption within these authorities.

5. Cost and Resource Intensiveness: Manual validation processes, including contacting issuing institutions or physically handling paper certificates, can be resource-intensive and costly. This is especially true for large-scale validation efforts or when dealing with a high volume of certificates.

6. Limited Transparency: Traditional methods often lack transparency in the validation process. Stakeholders may have limited visibility into the steps taken to verify a certificate, raising concerns about the reliability and accuracy of the validation outcome.

Addressing these challenges requires a shift towards more modern and technologically advanced validation methods, such as blockchain-based systems, to enhance security, efficiency, and standardization in the certificate validation process.

1.1.3 Benefits of Implementing Blockchain for Certificate Validation

1. Security and Immutability: Blockchain ensures the security and immutability of certificate records. Once a certificate is added to the blockchain, it cannot be altered or tampered with, providing a highly secure and trustworthy record of an individual's qualifications.

2. Decentralization: Blockchain operates in a decentralized manner, eliminating the need for a central authority to validate certificates. This decentralization enhances transparency, reduces the risk of single points of failure, and fosters trust among stakeholders.

3. Efficient Verification Processes: Smart contracts, and programmable scripts on the blockchain, can automate the verification process. This reduces the time and resources required for manual validation, providing a more efficient and streamlined approach.

4. Real-Time Access to Verified Information: Blockchain allows for real-time access to verified information. Stakeholders, such as employers or academic institutions, can quickly and securely validate certificates without relying on intermediaries, enhancing the overall speed of the validation process.

5. Enhanced Privacy Controls: Blockchain allows for the implementation of privacy-enhancing features. While ensuring transparency, it can also provide privacy controls, allowing individuals to share only the necessary details required for validation without compromising sensitive information.

6. Reduced Costs: Through automation, elimination of intermediaries, and increased efficiency, blockchain-based certificate validation can lead to cost reductions. Institutions and organizations can save resources traditionally spent on manual verification processes.

CHAPTER-2

LITERATURE SURVEY

2.1 Blockchain

Satoshi Nakamoto introduced the concept of blockchain in 2008, presenting it as an online ledger that facilitates decentralized and transparent data sharing. This innovative technology utilizes distributed ledgers where transaction data, housed in nodes, is compressed and appended to distinct blocks. Different types of data are dispersed across these blocks, allowing verifications to occur without the need for intermediaries. Through timestamps, all nodes collectively form a blockchain. Once information is entered into a block, it can be simultaneously verified and becomes immutable. This entire process is open to the public, ensuring transparency and security.

The introduction of Ethereum Smart Contracts in 2013 marked the evolution to blockchain 2.0. While blockchain 1.0, primarily employed by Bitcoin, addressed issues related to cryptocurrencies and decentralized payments, blockchain 2.0 aimed at decentralizing the entire market. It is now utilized to transform assets through smart contracts, introducing alternatives to Bitcoin Blockchain and creating new value.

2.2 Ethereum

Ethereum stands as an open and decentralized platform, boasting Turing completeness and supporting a diverse array of derivative applications. The majority of smart contracts and decentralized autonomous organizations are conceived and implemented using Ethereum. In comparison to Bitcoin blockchains functioning as a global payment network, Ethereum can be likened to a global computing system. Similar to Android, an open-source platform developed by Google, Ethereum serves as an infrastructure empowering developers to craft applications. This infrastructure is collaboratively developed and upheld by both the Ethereum platform itself and the contributing developers. The key attributes of Ethereum include:

Incorruptibility: Data remains unalterable, immune to tampering by third parties.

Security: Risks arising from human errors are mitigated as decentralized applications are maintained by entities rather than individuals.

Permanence: The blockchain persists without interruption, even in the event of individual computer or server failures[3].

2.2.1 Ethereum Virtual Machine (EVM)

The EVM is a programmable blockchain. Unlike Bitcoin, which provides a fixed set of commands, the EVM allows developers to run any programs in the manner they wish. Developers instruct the EVM to execute applications by using a high-level language called Solidity [2].

2.2.2 Solidity

Solidity is the programing language used for implementing smart contracts and is similar to JavaScript. After a Solidity-programmed smart contract is completed, a complier called solc is required to transform the Solidity code into contract bytecode, which is then interpreted by the EVM[2].

2.3 Smart Contracts

Nick Szabo first proposed the concept of smart contracts in the early 1990s, outlining their capability to enable computers to execute transaction clauses. With the increasing popularity of blockchain technology, smart contracts have gained heightened attention, particularly as a prominent feature of Ethereum, a blockchain platform established in 2015[2]. Defined as "digital contracts written in source code and executed by computers, integrating the tamper-proof mechanism of blockchain," smart contracts find application within the Ethereum blockchain.

Developers, based on their requirements, can specify instructions within smart contracts, creating diverse applications that interact with other contracts, store data, and facilitate Ether transfers. Deployed smart contracts are replicated to each node in the blockchain to prevent tampering. By automating operations through computers and leveraging Ethereum services, the likelihood of human error is diminished, reducing potential disputes.

Smart contracts find widespread use in voting systems and cryptocurrency applications. An illustration demonstrates how developers easily deploy smart contracts for cryptocurrency transactions. High-level programming languages such as Solidity, Serpent, and LLL are primarily employed for writing smart contracts[2]. Presently, Solidity is the language of choice for most developers who compile instructions into bytecode for execution.

CHAPTER-3

RESEARCH GAPS OF EXISTING METHODS

The limited research on achieving interoperability for blockchain-based certificate validation not only hampers the seamless exchange of information but also presents challenges to the scalability and sustainability of these systems. Furthermore, the lack of standardized protocols stifles innovation and impedes the full realization of advancements in certificate validation, obstructing the overall progress toward reliable and secure validation mechanisms. To effectively address these gaps, a collaborative approach involving researchers, industry stakeholders, and regulatory bodies becomes essential to establish standardized practices and promote a more cohesive and universally accepted framework in the certificate validation landscape.

The lack of comprehensive, long-term impact assessments for blockchain-based certificate validation systems highlights a significant research gap, emphasizing the need for a deeper understanding of their enduring implications. Conducting a thorough investigation into the sustained effectiveness of these systems becomes crucial for evaluating their reliability and performance over time, particularly in dynamic environments. Additionally, a critical aspect is the examination of scalability to determine whether these systems can efficiently handle a growing volume of certificates and users. Assessing the adaptability of blockchain-based certificate validation systems over an extended period is equally essential, given the rapid evolution of technology and the potential necessity for system updates to align with changing requirements. Research studies addressing these dimensions will provide invaluable insights into the feasibility and long-term viability of adopting blockchain for certificate validation on a broader scale.

Examining user experience aspects and potential challenges linked to the adoption of blockchain-based certificate validation systems is indispensable for their effective integration into real-world contexts. In-depth research in this realm should probe into end-users' perceptions and usability, considering factors like accessibility, user-friendliness, and overall satisfaction with the validation process. Equally vital is understanding the barriers encountered by end-users during implementation, providing valuable insights into areas necessitating improvement or additional support. Furthermore, delving into user feedback, concerns, and preferences will not only refine the design and functionality of blockchain-based certificate validation systems but also significantly contribute to enhancing user experience, ultimately fostering increased acceptance and adoption. Addressing these user-centric aspects is pivotal to ensure the seamless alignment of blockchain technology in certificate validation with user expectations and to effectively navigate any challenges that may arise.

Within the domain of certificate validation, a noticeable research gap exists in exploring hybrid approaches that seamlessly integrate blockchain technology with existing systems. Hybrid models, leveraging the strengths of both traditional and blockchain-based systems, hold the potential to provide pragmatic solutions for a gradual and efficient transition. Current research endeavors predominantly concentrate on standalone blockchain implementations, leaving a substantial void in understanding how these technologies can harmoniously coexist with legacy validation systems. As organizations contemplate the adoption of blockchain, it becomes imperative to develop methodologies for a smooth transition from traditional methods to blockchain-based systems. Research in this area should not only address the technical intricacies of integration but also encompass organizational and procedural considerations necessary for a successful and sustainable hybrid approach to certificate validation. Insights derived from such research will be invaluable in guiding institutions toward a seamless and effective adoption of blockchain technology within the intricate landscape of certificate validation.

The exponential growth of blockchain networks underscores the urgent need for research aimed at addressing scalability concerns, particularly concerning a substantial volume of certificate transactions. It is crucial to scale blockchain-based certificate validation systems to seamlessly accommodate an expanding user base and escalating transaction loads, ensuring their sustained effectiveness. In-depth research endeavors should explore cutting-edge solutions like sharding, layer-two implementations, and alternative consensus mechanisms to mitigate the challenges posed by scalability. For example, sharding entails dividing the blockchain into more manageable segments, facilitating parallel processing and augmenting overall throughput. A comprehensive investigation into the effectiveness and feasibility of these scalability solutions is vital to guarantee the long-term viability and efficient functioning of blockchain networks within the domain of certificate validation.

As concerns regarding the environmental impact of blockchain networks, particularly those relying on energy-intensive consensus mechanisms, continue to rise, there is a pressing need for more extensive research exploration. It is crucial to delve into sustainable approaches that can effectively mitigate the carbon footprint associated with blockchain-based certificate validation systems. This research should specifically focus on developing energy-efficient consensus mechanisms and exploring alternatives that prioritize environmental sustainability while maintaining the security and integrity of the validation process. Additionally, examining the incorporation of renewable energy sources within blockchain networks can significantly contribute to reducing their overall environmental impact. By addressing these dimensions, research can play a crucial role in promoting environmentally responsible practices within the domain of blockchain-based certificate validation.

Enhancing privacy in blockchain-based certificate validation necessitates a thorough exploration of advanced privacy-preserving mechanisms, an area currently lacking in-depth research. To bolster user privacy and confidentiality, further investigation is needed into innovative approaches that leverage cryptographic techniques and privacy-centric smart contract designs. The research should concentrate on developing robust encryption methods to secure sensitive certificate information within the blockchain framework. Moreover, meticulous attention is required in designing privacy-focused smart contracts, striking a delicate balance between protecting individual data and maintaining the transparency and verifiability intrinsic to blockchain transactions. By channeling research efforts into these areas, the blockchain community can actively contribute to the advancement of more secure and privacy-conscious certificate validation systems.

The insufficiency of research on regulatory challenges and frameworks compliant with blockchain-based certificate validation underscores a significant gap in understanding and addressing legal and regulatory considerations. To bridge this void, research efforts should be channeled into gaining comprehensive insights into the dynamic nature of regulatory landscapes and their implications for blockchain implementations. This entails not only grasping current regulations but also proactively anticipating and adapting to regulatory changes that could impact the validation processes. Additionally, investigating methods to seamlessly integrate compliance measures into blockchain-based certificate validation systems is pivotal for building trust and promoting widespread adoption.

The influence of blockchain-based certificate validation on educational pedagogy represents a relatively unexplored domain, prompting the need for extensive research to uncover its implications. Understanding how the adoption of blockchain technology shapes teaching methodologies is paramount, as it may introduce innovative approaches to credential verification and authentication within educational institutions. Exploring the impact on student engagement becomes crucial, given that blockchain has the potential to enhance trust and credibility associated with certificates, thereby fostering a more engaged and motivated student body. Additionally, delving into the overall learning experience within the context of blockchain adoption can yield insights into potential shifts in the educational landscape, offering valuable perspectives for educators, institutions, and policymakers aiming to leverage emerging technologies for pedagogical advancements. Through dedicated research efforts at the intersection of blockchain and education, a deeper comprehension of its transformative potential can be attained, paving the way for informed and innovative educational practices.

The advancement of cross-border validation and mutual recognition of certificates using blockchain technology is a research area that requires heightened attention. A thorough exploration is essential to comprehend and tackle the intricacies involved in formulating international standards and protocols for seamless cross-border validation. Research endeavors should concentrate on constructing a framework that not only guarantees the authenticity and integrity of certificates across borders but also nurtures trust and collaboration among diverse educational and professional entities. Delving into the legal, regulatory, and technological facets of cross-border certificate validation becomes imperative to establish a sturdy foundation for international cooperation in credential verification. By giving precedence to research in this domain, the blockchain community can actively contribute to the creation of a globally recognized and interoperable system that transcends geographical boundaries, providing benefits to individuals, institutions, and employers on a global scale.

While smart contracts have proven valuable in static certificate validation, their largely unexplored potential in dynamic credentialing, especially for continuous learning achievements, necessitates thorough investigation. Research endeavors should extensively examine how smart contracts can be applied to streamline and record ongoing skills development, fostering a more adaptable and responsive credentialing process. The exploration of integrating smart contracts with real-time learning platforms and achievements holds promise for achieving a transparent and automated validation of evolving skill sets.

Moreover, a critical aspect involves comprehending the legal and regulatory considerations associated with deploying smart contracts in dynamic credentialing scenarios to establish a secure and compliant framework. By concentrating on these facets, research has the potential to unveil innovative approaches to credentialing that align with the ever-changing nature of skills in the digital era.

The examination of social and ethical implications in the realm of blockchain-based certificate validation is an underexplored domain, necessitating thorough research to uncover issues related to inequality, access, and potential biases inherent in the validation process. It is imperative to investigate how blockchain implementations might inadvertently worsen existing societal inequalities or introduce new disparities, promoting the development of an inclusive and equitable certification ecosystem. A crucial aspect involves scrutinizing the accessibility dimensions of blockchain-based validation systems to guarantee that individuals, regardless of socio-economic factors or technological literacy, can equally access and engage in the validation process. Additionally, understanding the potential biases embedded in the algorithms or decision-making processes within blockchain validation is essential for mitigating unintentional discriminatory effects.

CHAPTER-4

PROPOSED METHODOLOGY

The outlined blockchain-based certificate validation system features a comprehensive architecture meticulously crafted to enhance security, transparency, and operational efficiency in the validation process.

At its foundation, the system capitalizes on a decentralized blockchain network, deploying nodes strategically distributed across the network to collectively oversee and authenticate certificates. Each certificate undergoes cryptographic hashing, generating a distinctive identifier stored within a blockchain block. Smart contracts play a pivotal role, automating validation procedures and streamlining the process, thereby diminishing the reliance on manual verification.

Privacy is a paramount consideration in this proposed architecture, with a focus on selective disclosure. This empowers individuals to govern the information divulged during the validation process. Furthermore, the system incorporates mechanisms for real-time updates to certificates, ensuring stakeholders have immediate access to the most up-to-date and precise information.

The architecture stands out for its attributes of adaptability, scalability, and a steadfast commitment to revolutionizing certificate validation through pioneering blockchain technologies. The steps involved are.

At backend:

a) Setting up an Ethereum Test network.

b) Adding ETH to a digital wallet to communicate with the Ethereum network.

c) Preparing smart Contracts using Solidity.

d) Deployment of Smart Contract to Test Network.

At frontend:

a) We will be using the Material UI package for designing our website.

b) For Connecting the Front end and Backend we will be using WEB 3 APIs.

Use cases Referred

There are 4 main Use Cases:

a) Registering Institutes by Central Authority] (Use-Case-1-Registering-Institutes)

b) Issuing Certificates by Institutes] (Use-Case-2-Issuing-Certificates)

c) Revoking Certificates by Institutes] (Use-Case-3-Revoking-Certificates)

d) Viewing Certificates by Employers/Public] (Use-Case-4-Viewing-Certificates)

Technologies and frameworks used for implementation.

Software details:

a) Prerequisites:

- Basic Knowledge of blockchain [Ethereum]
- Working of dapp [decentralized application]
- Solidity language
- Web3 API
- Infura API and associated test nets.
- Ganache software

b) Software Used:

- Truffle IDE for smart contract implementation.
- Visual Studio Code IDE
- React JS framework
- Node JS and npm-v16
- Metamask account for setting up a digital wallet for storing eth
- Solidity language installation for creating Smart Contract
- Ganache software for testing purposes.
- Material UI package for designing purposes.

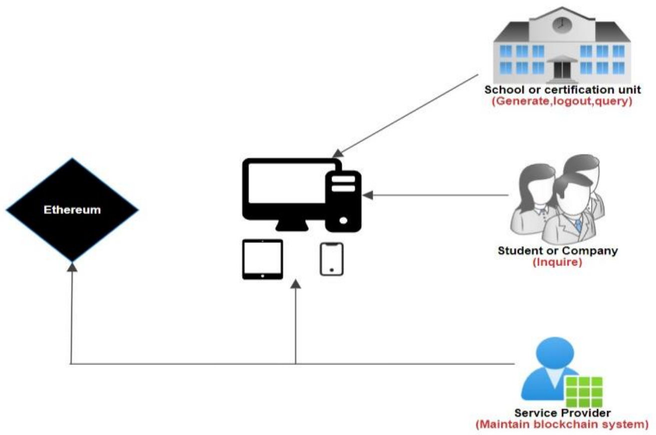


Figure 4.1 – Interaction among actors

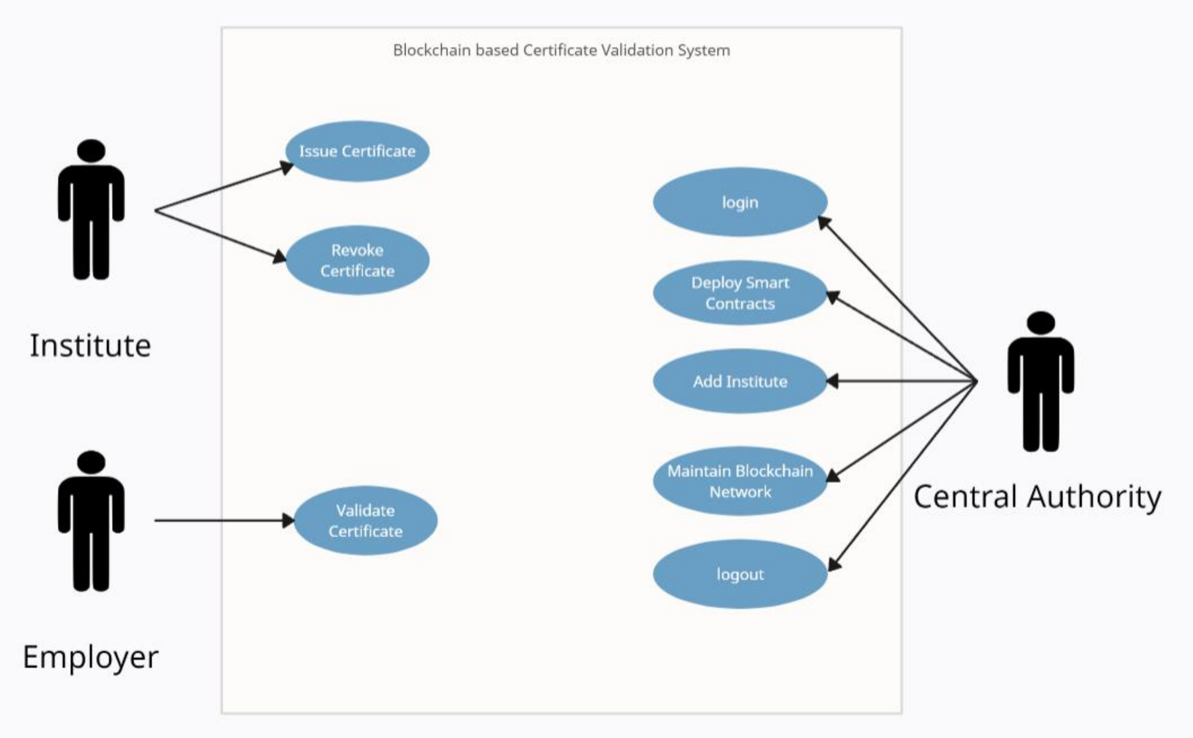


Figure 4.2 – Use case Diagram

The certificate submission process within the proposed system is designed to be a systematic and secure journey for users and issuers. It initiates with user registration, where individuals provide necessary details for identity verification. This step ensures that the platform maintains a secure user base with verified identities. Following this, certificate issuers, such as educational institutions, take charge of the certificate issuance request. During this phase, they submit relevant details, including recipient information, qualifications, and other necessary attributes.

The submitted certificate data then undergoes a critical step of cryptographic hashing and encryption. Cryptographic hashing generates a unique hash for each certificate, contributing to its integrity and security. Additionally, sensitive information may be encrypted to enhance privacy, ensuring that only authorized parties can access certain details. The core of the validation process lies in the execution of a smart contract, where predefined criteria, such as issuer authorization and format compliance, are rigorously checked. Once validated, the hashed and encrypted certificate data, along with issuance details, is recorded as a transaction on the blockchain. This transaction, being time-stamped and including relevant metadata, adds an extra layer of transparency and tamper-proofing to the certificate issuance process. Subsequently, certificate holders receive notifications confirming the successful issuance and recording of their certificates on the blockchain, ensuring they are well-informed and can trust the integrity of their digital credentials.

The certificate validation phase, on the other hand, involves a seamless user authentication process where validators and certificate holders log in securely. Certificate holders then submit their certificates for validation through the user interface. The submitted certificate data goes through the same cryptographic hashing and encryption processes for validation, ensuring that the certificate's integrity is maintained throughout its lifecycle. A dedicated smart contract designed for validation is then executed. This smart contract rigorously checks the validity of the submitted certificate against predefined criteria, including expiration date, issuer authenticity, and accreditation status. The end result is a comprehensive and secure system that leverages advanced technologies like blockchain and smart contracts to optimize both the submission and validation processes, ensuring a secure, transparent, and efficient certificate management system.

The certificate submission and verification processes are meticulously outlined to ensure a systematic, secure, and auditable experience within the proposed blockchain-based system. Certificate holders begin by logging in or registering on the platform, gaining access to their personalized dashboards where they can seamlessly submit new certificates or review existing ones. The submitted data undergoes a critical phase of processing, including hashing and encryption, aimed at generating a unique hash for the certificate data and optionally encrypting sensitive information within the certificate. For added validation rigor, smart contracts may be executed to validate submissions against predefined rules and criteria.

On the verification side, validators, upon secure authentication, access their dashboards listing certificates pending validation. They select a certificate for verification, and the platform retrieves the hashed certificate data from the blockchain. The verification process involves additional hashing and encryption steps, where the submitted certificate data is processed to generate a hash for validation. If the certificate was encrypted during submission, optional decryption occurs at this stage. The smart contract queries the blockchain to retrieve the recorded hash of the original certificate and proceeds with a thorough validation comparison. This includes checking against various predefined criteria such as expiration date, accreditation status, and issuer authenticity.

The result of the validation is promptly determined, and certificate holders receive real-time notifications indicating the status of their certificates. Optionally, certificate issuers may also be notified of successful validations. Crucially, the validation result is recorded as a transaction on the blockchain, creating a transparent and tamper-proof audit trail of the entire validation process.

In terms of instant and reliable verification results presentation, the system leverages the efficiency of blockchain and smart contracts to automate the validation process. Users experience real-time feedback, with verification outcomes instantly displayed in a clear and concise manner. The user interface employs comprehensible status updates, clearly confirming the validity of the certificate or providing specific details in case of discrepancies. Visual indicators enhance user understanding, accelerating the validation process and fostering confidence in the system's accuracy and reliability. This emphasis on immediate and reliable result presentation is a key feature contributing to the overall effectiveness and user trust within the proposed certificate validation system, providing stakeholders with swift access to crucial information for educational or professional purposes.

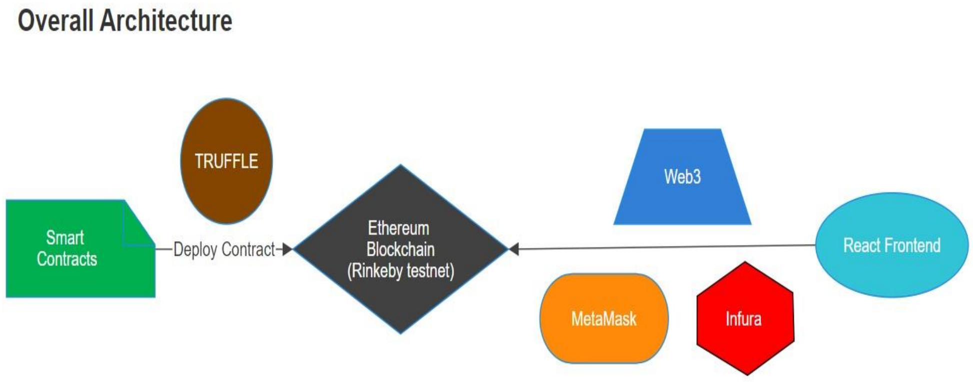


Figure 4.3 – Architectural Diagram

CHAPTER-5

OBJECTIVES

1. To enhance security, deploy advanced cryptographic techniques and leverage blockchain technology to fortify the security and integrity of certificate data. To achieve this, employ cryptographic hashing and encryption mechanisms to ensure that certificate information remains secure and tamper-proof. The implementation of these techniques aims to prevent unauthorized access, tampering, or forgery of certificates, providing robust security measures throughout the entire validation process.

2. To enhance efficiency and streamline processes, integrate smart contracts and automation to simplify the traditionally cumbersome certificate submission and validation processes. By leveraging smart contracts, the system can automate the verification steps, reducing the need for manual intervention and expediting the validation workflow.

3. To prioritize user privacy, implement mechanisms that empower individuals to exercise control over the information shared during the validation process. To achieve this, incorporate selective disclosure features, allowing users to disclose only necessary information while keeping sensitive details confidential. Additionally, this approach aligns with evolving privacy regulations and standards, contributing to a user-centric validation system that respects and safeguards personal information.

4. To facilitate real-time updates and notifications, the system is designed to offer stakeholders, including certificate holders and issuers, immediate information on the status of certificates. Implementing real-time notifications ensures that relevant parties receive instant updates upon successful validation, fostering timely communication. This proactive approach not only keeps certificate holders informed about the current status of their credentials but also enables issuers to stay abreast of the validation outcomes in real-time.

5. To achieve adaptability and scalability, the system should be built upon a flexible

architecture capable of evolving with changing requirements and scaling to handle an increasing volume of certificates. This adaptable design ensures seamless integration with existing systems, allowing for a smooth transition without disrupting established processes. Moreover, by incorporating modular components and open standards, the system can easily accommodate future technological advancements, positioning itself as a resilient and future-proof solution.

6. To establish a tamper-proof ledger of certificate submission and validation. By utilizing the decentralized and transparent nature of blockchain, the system creates an immutable record that serves as an auditable trail of all certificate transactions. This not only enhances trust among stakeholders but also provides a clear and traceable history of every step in the validation process.

7. To provide a positive user experience, the system is designed with an intuitive and user-friendly interface, catering to both certificate holders and validators. The aim is to create a platform where stakeholders can seamlessly navigate, submit or validate certificates, and access relevant information effortlessly.

8. To guarantee the system's operation within legal and ethical boundaries, ensure strict adherence to relevant regulations and legal frameworks governing certificate issuance and validation. This involves a comprehensive approach to address data protection laws and industry-specific compliance requirements.

9. To stay at the forefront of advancements in the field, the system is committed to innovation by revolutionizing traditional certificate validation methods through the integration of cutting-edge blockchain technologies. By embracing innovation, the system seeks to offer a dynamic and future-proof approach to certificate validation.

CHAPTER-6

SYSTEM DESIGN & IMPLEMENTATION

Designing and implementing a blockchain-based certificate validation system involves a comprehensive approach, encompassing system architecture, smart contract development, user interface design, and integration with blockchain technology. Below is an overview of the key components and steps involved in the system design and implementation:

1. System Architecture:

   a) Decentralized Blockchain Network: Establish a decentralized blockchain network using a suitable blockchain platform (e.g., Ethereum, Hyperledger). This network will serve as the foundation for recording and validating certificate transactions.

   b) Nodes and Consensus Mechanism: Set up nodes to participate in the blockchain network, ensuring decentralization. Define a consensus mechanism for reaching agreement on the validity of transactions.

2. Smart Contract Development:

   a) Certificate Issuance Smart Contract: Develop a smart contract responsible for handling the certificate issuance process. This contract should include logic for validating issuance requests, generating unique identifiers (hashes), and recording transactions on the blockchain.

   b) Certificate Validation Smart Contract: Create a separate smart contract dedicated to the validation process. This contract should verify the authenticity of certificates based on predefined criteria and record validation outcomes on the blockchain.

3. User Authentication and Authorization:

   a) User Registration and Login: Implement a secure user registration and login system to authenticate users on the platform. Users, including certificate holders and validators, should have unique login credentials to access their respective dashboards.

   b) Role-Based Access Control: Define roles and permissions for different user types (certificate holders, validators, administrators). Ensure that each role has specific access privileges within the system.

4. User Interface Design:
   1. a) Dashboard for Certificate Holders: Design an intuitive dashboard for certificate holders to submit new certificates, view existing ones, and receive real-time updates on the status of their certificates.
   2. b) Dashboard for Validators: Create a dashboard for validators to access certificates pending validation, select certificates for verification, and view detailed validation results.
   3. c) Notification System: Implement a notification system to alert users about the status of their certificates, providing instant feedback on the validation outcome.

5. Privacy and Security Measures:
   1. a) Selective Disclosure Mechanisms: Integrate mechanisms for selective disclosure to enhance user privacy during the validation process. Allow users to control the information shared with validators.
   2. b) Encryption: Implement encryption techniques to safeguard sensitive information within certificates, ensuring that only authorized parties can access specific details.

6. Integration with Blockchain:
   1. a) Blockchain API Integration: Integrate the developed smart contracts with the chosen blockchain platform using appropriate APIs. Ensure seamless communication between the system and the blockchain network.
   2. b) Transaction Handling: Implement logic for handling blockchain transactions, including submitting new certificates, updating validation status, and querying certificate data.

7. Testing and Quality Assurance:
   1. a) Unit Testing: Conduct thorough unit testing for each component, including smart contracts, user interfaces, and backend logic.
   2. b) Integration Testing: Test the integration of different system components to ensure seamless functionality.
   3. c) Security Audits: Perform security audits to identify and address potential vulnerabilities in the system.

8. Deployment and Maintenance:
   a) Deployment Strategy: Choose an appropriate deployment strategy for the system, whether on a cloud platform or on-premises. Ensure scalability and reliability.
   b) Monitoring and Maintenance: Implement monitoring tools to track system performance, detect anomalies, and address any issues promptly. Establish a maintenance plan for regular updates and improvements.

By following these steps, the system can be designed and implemented to effectively validate certificates using blockchain technology while ensuring security, privacy, and user-friendly interactions. Continuous monitoring and updates will contribute to the long-term success and reliability of the blockchain-based certificate validation system.

6.1 USECASE DIAGRAMS :

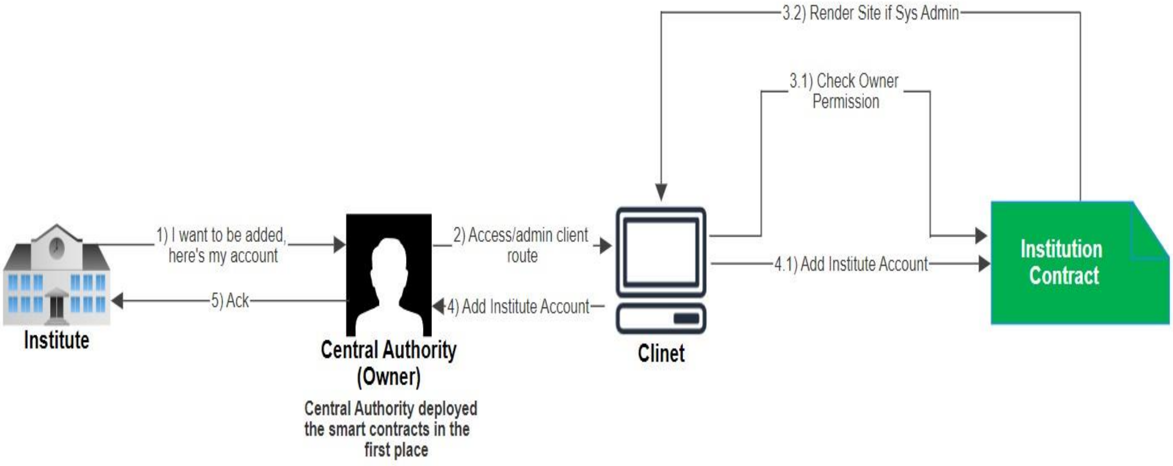

3.2) Render Site if Sys Admin
3.1) Check Owner Permission
1) I want to be added, here's my account
2) Access/admin client route
5) Ack
4) Add Institute Account
4.1) Add Institute Account
Institution Contract
Institute
Central Authority (Owner)
Central Authority deployed the smart contracts in the first place
Clinet

Figure 6.1 – Use case diagram for Adding Institutes

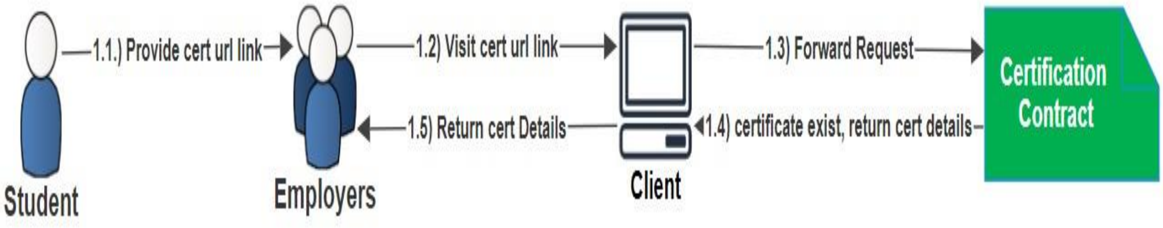


Figure 6.2 – Use case diagram for Viewing Certificates

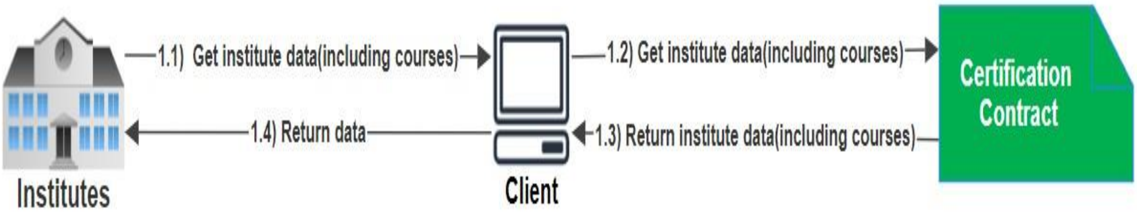

1.1) Get institute data(including courses)
1.4) Return data
Institutes
Client
1.2) Get institute data(including courses)
1.3) Return institute data(including courses)
Certification Contract

Figure 6.3 – Use case diagram for Getting Course Details

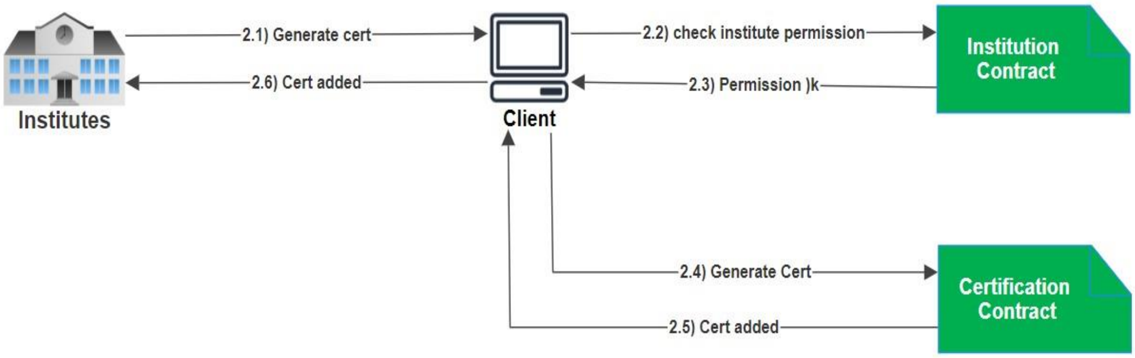


Figure 6.4 – Use case diagram for Generating Certificates

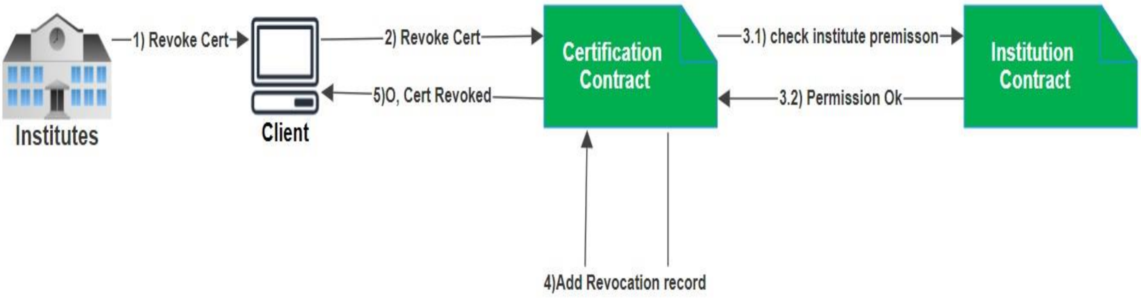
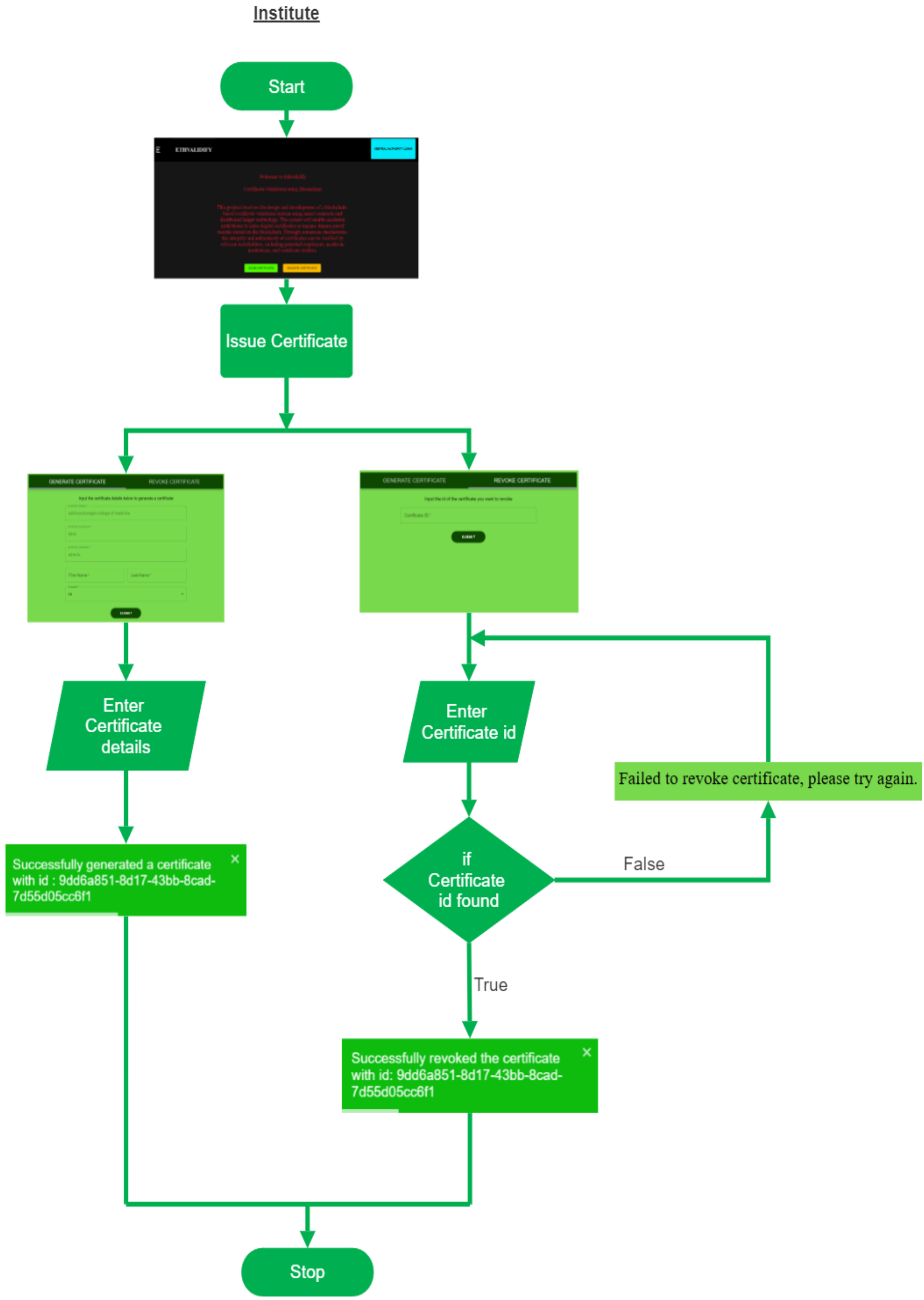


Figure 6.5 – Use case diagram for Revoking Certificates



This project involves the design and development of a blockchain-based certificate validation system using smart contracts and distributed ledger technology. The system will enable academic institutions to issue digital certificates as tamper-proof records stored on the blockchain. Through consensus mechanisms, the integrity and authenticity of certificates can be verified by relevant stakeholders, including potential employers, academic institutions, and certificate holders.

Successfully generated a certificate with id : 9dd6a851-8d17-43bb-8cad-7d55d05cc6f1 ×

Failed to revoke certificate, please try again.

Successfully revoked the certificate with id: 9dd6a851-8d17-43bb-8cad-7d55d05cc6f1 ×

Figure 6.6 – Flow Diagram for Institute Portal (*with Screenshots provided*)

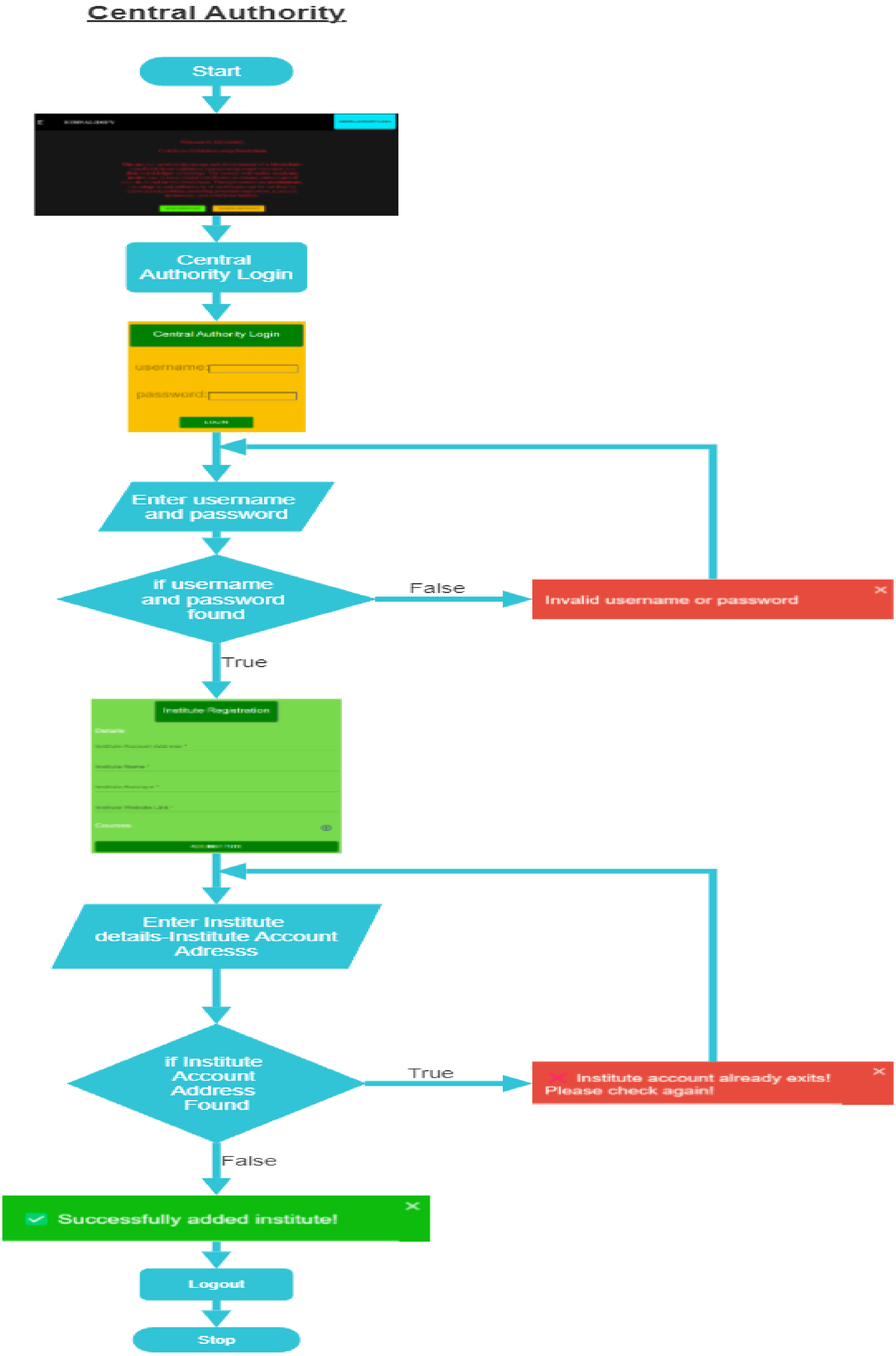
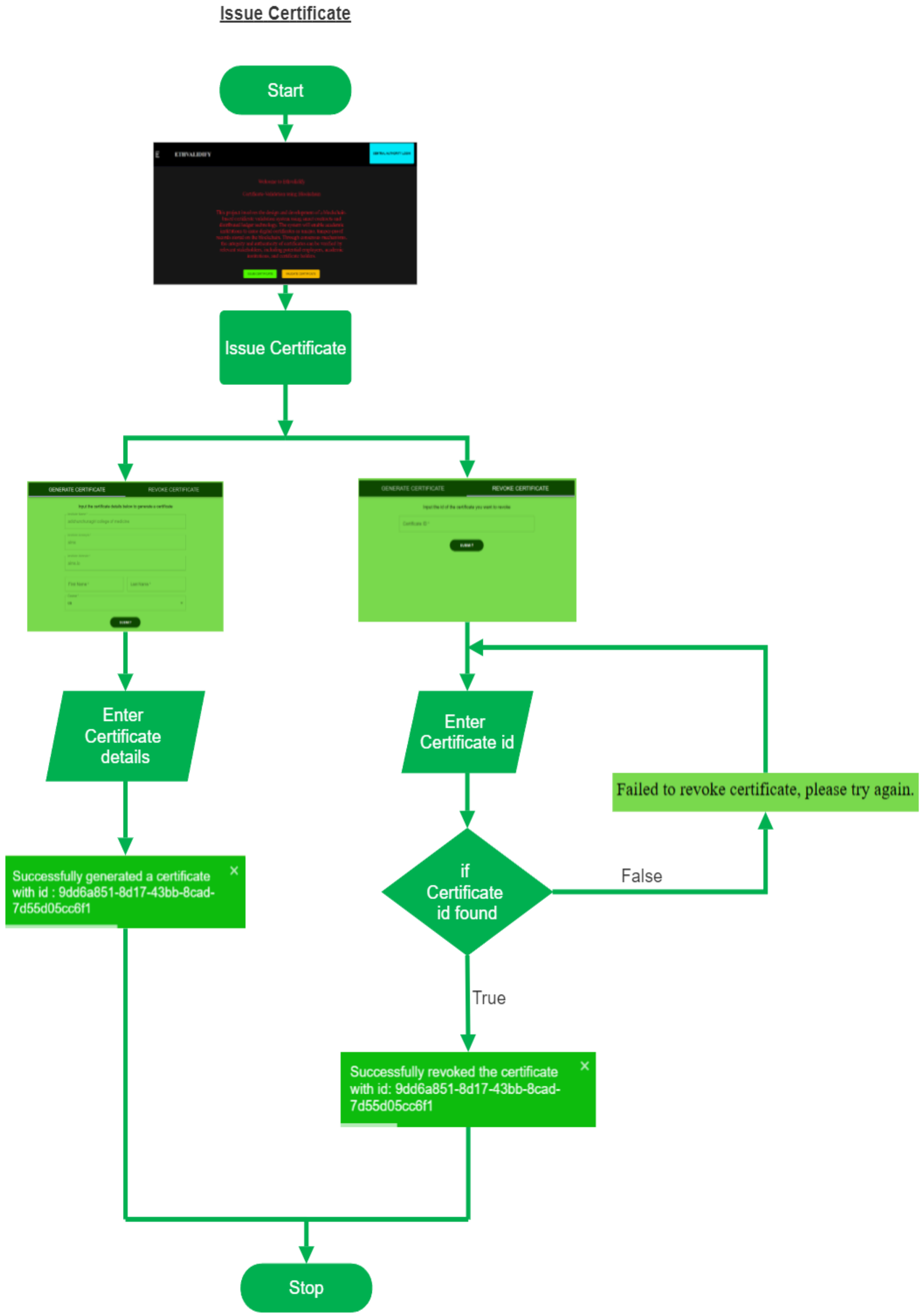

Central Authority
Start
Central Authority Login
Central Authority Login
username:
password:
LOGIN
Enter username and password
if username and password found
False
Invalid username or password
True
Institute Registration
Details
Courses
Enter Institute details-Institute Account Adresss
if Institute Account Address Found
True
Institute account already exits! Please check again!
False
Successfully added institute!
Logout
Stop

Figure 6.7 – Flow Diagram for Central Authority Portal (*with Screenshots provided*)



Failed to revoke certificate, please try again.

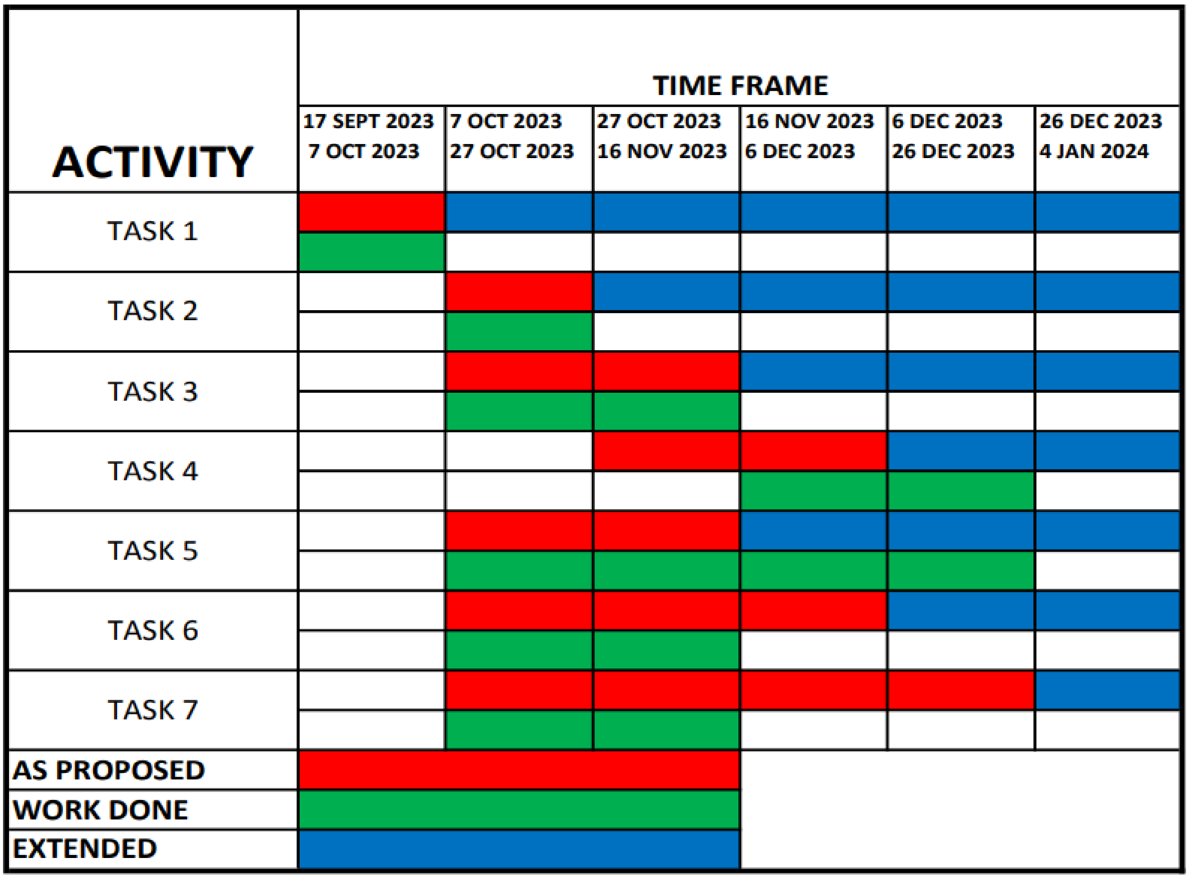
Successfully generated a certificate with id : 9dd6a851-8d17-43bb-8cad-7d55d05cc6f1

Successfully revoked the certificate with id: 9dd6a851-8d17-43bb-8cad-7d55d05cc6f1

Figure 6.8 – Flow Diagram for Employer Portal (*with Screenshots provided*)

CHAPTER-7

TIMELINE FOR EXECUTION OF PROJECT



ACTIVITY	TIME FRAME					
	17 SEPT 2023 7 OCT 2023	7 OCT 2023 27 OCT 2023	27 OCT 2023 16 NOV 2023	16 NOV 2023 6 DEC 2023	6 DEC 2023 26 DEC 2023	26 DEC 2023 4 JAN 2024
TASK 1	🟥	🟦	🟦	🟦	🟦	🟦
	🟩					
TASK 2		🟥	🟦	🟦	🟦	🟦
		🟩				
TASK 3		🟥	🟥	🟦	🟦	🟦
		🟩	🟩			
TASK 4			🟥	🟥	🟦	🟦
				🟩	🟩	
TASK 5		🟥	🟥	🟦	🟦	🟦
		🟩	🟩	🟩	🟩	
TASK 6		🟥	🟥	🟥	🟦	🟦
		🟩	🟩			
TASK 7		🟥	🟥	🟥	🟥	🟦
		🟩	🟩			
AS PROPOSED	🟥					
WORK DONE	🟩					
EXTENDED	🟦					

Figure 7.1 – Gantt chart

Task 1- To define project objectives and Scopes
Task 2- Identify the Use Cases
Task 3-Create Data Structures and Smart Contracts
Task 4-Create architecture and data flow diagrams
Task 5-User Interface Design
Task 6-Back-end Design
Task 7-Front-end Design

The timeline for the execution of a blockchain-based certificate validation project can vary depending on factors such as project scope, complexity, team size, and available resources.

Below is a general timeline broken down into key phases:

1. Project Planning (20 days):
   a) Define project objectives, scope, and requirements.

   b) Conduct feasibility studies.

   c) Create a detailed project plan, including tasks, milestones, and resource allocation.

   d) Identify potential risks and develop mitigation strategies.

2. System Planning and Use Case Identification (Month 3-4)

   a) Identify use cases and outline data structures.

   b) Conduct workshops or interviews to elicit and document use cases.

   c) Collaborate with stakeholders to prioritize use cases based on business value.

   d) Begin the high-level design of data structures and relationships.

   e) Initiate discussions on privacy and security considerations.

3. Data Structures and Smart Contracts Development (Month 5-8):

   a) Create data structures and develop smart contracts.

   b) Refine and finalize data structures based on use case requirements.

   c) Develop and test smart contracts for certificate issuance and validation.

   d) Implement cryptographic hashing and encryption for data security.

   e) Ensure compliance with blockchain platform standards.

4. System Architecture and Data Flow Diagrams (Month 9-10):

   a) Define system architecture and illustrate data flow.

   b) Collaborate with system architects to design the overall system architecture.

   c) Create detailed data flow diagrams highlighting information exchange.

   d) Identify key components, interfaces, and dependencies within the system.

   e) Conduct reviews with technical and non-technical stakeholders for feedback.

5. User Interface Design (Month 11-12):

   a) Design user interfaces for different stakeholders.

   b) Collaborate with UX/UI designers to create wireframes and prototypes.

   c) Incorporate feedback from end-users and stakeholders to refine designs.

   d) Ensure accessibility and usability standards are met.

   e) Develop design specifications for front-end development.

6. Back-end Design (Month 13-14):
   a) Design the back-end infrastructure and database.
   b) Define database schema and relationships based on data requirements.
   c) Choose appropriate database technologies for scalability and performance.
   d) Integrate back-end components with the chosen blockchain network.
   e) Design APIs and middleware for seamless communication between front-end and back-end.

7. Front-end Design (Month 15-16):
   a) Implement front-end design based on user interfaces.
   b) Develop responsive and interactive front-end components.
   c) Integrate front-end with back-end APIs and blockchain functionalities.
   d) Implement user authentication and authorization mechanisms.
   e) Conduct usability testing to ensure a positive user experience.

These detailed activities provide a more granular view of the tasks and considerations involved in each project phase. Adjustments may be needed based on project specifics and feedback received during the iterative development process.

It's important to note that these timelines are approximate, and the actual duration may vary based on project-specific factors. Regular communication, agile development practices, and flexibility in adapting to changing requirements can contribute to the successful execution of the project within the proposed timeline.

CHAPTER-8

OUTCOMES

- We have Successfully developed a blockchain-based certificate validation system utilizing the Ethereum network. Smart contracts are deployed and utilized for certificate issuance, validation, and revocation.
- Implementation of role-based access control for different actors (Central Authority, Employers, and Institutes) within the system. Each actor has specific privileges and permissions regarding certificate validation.
- Central Authority Functions:

  Issuance and Verification: The Central Authority can issue certificates and verify the authenticity of certificates issued by institutes.

  Revocation: Ability for the Central Authority to revoke certificates in case of fraud.
- Institutes Functions:

  Certificate Issuance: Institutes can issue certificates to candidates upon successful Completion of program.

  Data Integrity: Ensuring data integrity by storing certificate details securely on the Blockchain.
- Employers Functions

  Certificate Verification: Ability for employers to verify the authenticity and validity of certificates presented by job applicants.

  Trust and Transparency: Increased trust and transparency in hiring processes through verified certificates.
- Successful integration of MetaMask for secure transactions and user authentication. Utilization of Infura for seamless connection to the Ethereum network.
- Creation of a user-friendly and intuitive interface using ReactJS for the DApp. Interface includes features for certificate issuance, verification, and revocation by different actors.
- Improved security through blockchain's immutable and decentralized nature, ensuring tamper-proof certificates. Establishment of trust among stakeholders due to the transparent and verifiable nature of the certificate validation process.
- Design and implementation of a scalable system capable of handling a growing number of certificates and users efficiently.

- Conducting user education sessions to familiarize all actors (Central Authority, Institutes and Employers) with the system's functionalities and advantages. Encouraging widespread adoption of the blockchain-based certificate validation system.

CHAPTER-9

RESULTS AND DISCUSSIONS

9.1 Results:

9.1.1 Technical Implementation:

- **Blockchain Integration:**

  Successfully deployed smart contracts for certificate validation on the Ethereum network using Infura for connectivity.

  Implemented smart contract functions for certificate issuance, validation, and revocation.
- **MetaMask Integration:**

  Integrated MetaMask for secure and seamless currency transfer within the application.
- **DApp Interface:**

  Created an intuitive and user-friendly interface using ReactJS for Central Authority, Employers, and Institutes to interact with the system.

9.1.2 Functionality Testing:

- **Certificate Operations:** Issuance of certificates by Institutes verified by Central Authority. Employers successfully validated certificates for authenticity. The revocation process was tested and validated, ensuring proper handling of revoked certificates.
- **Actor Interactions:** Central Authority effectively managed certificate validation tasks. Institutes issued certificates adhering to defined protocols. Employers seamlessly verified certificates with blockchain validation.

9.1.3 User Interface Evaluation:

- **Usability and Experience**: Conducted usability tests ensuring a smooth user experience across all actor roles. Addressed UI/UX issues based on user feedback, enhancing accessibility and navigation.

9.2 Discussion:

9.2.1 System Performance:

- Speed and Scalability: Analyzed transaction speed and scalability concerning peak usage scenarios. Considered potential bottlenecks and scalability challenges for future improvements.

9.2.2 Security and Trustworthiness:

- Block chain Security: Explored the immutability of blockchain ensuring tamper-proof certificate records. Discussed the decentralized nature of the system, fostering trust among stakeholders.

9.2.3 Impact on Stakeholders:

- Benefits to Actors: Central Authority experienced improved validation efficiency and transparency. Employers gained trust in validated certificates, reducing verification complexities. Institutes provided more reliable and easily verifiable certificates to students/employees.

9.2.4 Technical Challenges and Future Improvements:

- Challenges Encountered: Addressed challenges related to gas fees, network congestion, and contract deployment delays.
- Future Enhancements: Proposed optimizations to enhance transaction speed, reduce costs, and improve user experience. Considered the addition of features like batch verification for Employers and advanced analytics for Central Authority.

CHAPTER-10
CONCLUSION

The infusion of blockchain technology into certificate validation has showcased tremendous promise in reshaping conventional credential verification methods. After a thorough exploration and analysis of various blockchain platforms, was carefully chosen as the cornerstone for crafting a resilient and dependable certificate validation system.

The project's outcomes have proven highly encouraging, resulting in a prototype that marks the level of security, transparency, and reliability throughout the certificate validation journey. Its potential to disrupt age-old validation practices across sectors like education, professional certifications, and legal documentation is evident, fostering enhanced trust and efficiency in verifying credentials. Blockchain technology prominently features robust data security. Serving as an expansive and accessible online ledger, each node securely stores and validates identical data. The implementation of the suggested blockchain-based system significantly lowers the risk of certificate forgery. Within the system, both the certificate application process and automated certificate granting are conducted openly and transparently. Companies or organizations have the capability to request information on any certificate directly from the system.

In summary, this project signifies a significant leap towards refining the validation process by leveraging blockchain technology. The progress achieved underscores the transformative potential of blockchain in upholding the integrity and genuineness of certificates, paving the way for a more secure and trustworthy environment for verifying credentials. The utilization of the suggested blockchain-based system significantly diminishes the risk of certificate forgery. The system ensures transparency in the certificate application and automated certificate granting processes, allowing companies or organizations to readily access information on any certificate.

REFERENCES

[1] S. Yao, J. Chen, K. He, R. Du, T. Zhu, and X. Chen, "PBCert: Privacy-Preserving Blockchain-Based Certificate Status Validation Toward Mass Storage Management," in IEEE Access, vol. 7, pp. 6117-6128, 2019, doi: 10.1109/ACCESS.2018.2889898.

[2] J. Cheng, N. Lee, C. Chi, and Y. Chen, "Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, 2018, pp. 1046-1051, doi: 10.1109/ICASI.2018.8394455.

[3] Rohan Hargude, Ghule Ashutosh, Abhijit Nawale, Sharad Adsure,” Validation and verification of certificates using Blockchain”, 2021 IJCRT | Volume 9, Issue 6 June 2021 | ISSN: 2320-2882.

[4] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere and B. Stiller, The Proposal of a Blockchain-based

[5] Architecture for Transparent Certificate Handling, BIS2018: Business Information System. Workshops

[6] Gayathiri, A., Jayachitra, J., & Matilda, S (2020). Certificate validation using blockchain. 2020

[7] Sarah, Kamalesh, Chamon, Quek, “Web 3.0 and a Decentralized Approach to education” in arXiv.org DOI:19 Dec 2023

[8] M Abubakar,McCarron Edinburgh Napier University,” Blockcahin-based Platform for Secure Sharing and Validation of Vaccination Certificates” in IEEExplore DOI: 10.1109/SIN54109.2021.9699221

[9] L Marchesi, M Marchrsi, Roberto DMI university, “A Blockchain Architecture for Industrial Applications” Research gate DOI:10.1016/j.bcra.2022.100088

[10] Shanmuga Priya, Swetha N, “Online Certificate Validation Using Blockchain” Special Issue Published in Int. Jnl. Of Advanced Networking & Applications (IJANA).

[11] V jayashankara Acharya, K Mahanthi, “Validation and Verification of Blockchain Based Digital Certificate”, Industrial Engineering Journal ISSN: 0970-2555 Volume : 52, Issue 7, July : 2023

[12] Xiuping Lin, “Semi-centralized Blockchain SmartContracts: Centralized Verification and SmartComputing under Chains in theEthereumBlockchain”,Department of Information Engineering, National Taiwan University, Taiwan,R.O.C., 2017.

[13] Yong Shi, “Secure storage service of electronicballot system based on block chain algorithm”,Department of Computer Science, Tsing HuaUniversity, Taiwan, R.O.C., 2017.

[14] ZhenzhiQiu, “Digital certificate for a painting basedon blockchain technology”, Department ofInformation and Finance Management, NationalTaipei University of Technology, Taiwan, R.O.C.,2017

APPENDIX-A

PSEUDOCODE

1. Contract Certification

```
State Variables:
    owner: address
    institution: Institution
    certificates: mapping(bytes32 => Certificate)

Events:
    certificateGenerated(bytes32 _certificateId)
    certificateRevoked(bytes32 _certificateId)

Constructor:
    Certification(Institution _institution)
        owner = msg.sender
        institution = _institution

Struct Certificate:
    candidate_name: string
    course_name: string
    creation_date: string
    institute_name: string
    institute_acronym: string
    institute_link: string
    revoked: bool

Function stringToBytes32:
    Convert string to bytes32

Function generateCertificate:
    Inputs: string _id, string _candidate_name, uint256 _course_index, string _creation_date
    Validate institute permission
    Convert _id to bytes32
    Check if the certificate with _id already exists
    Retrieve institute data using the institute address
    Validate course index
    Get course name from institute courses array
    Set revocation status to false
    Create a certificate and emit certificate generated event

Function getData:
    Inputs: string _id
    Convert _id to bytes32
    Check if the certificate with _id exists
    Retrieve certificate data
    Return certificate details

Function revokeCertificate:
    Inputs: string _id
    Validate institute permission
    Convert _id to bytes32
    Check if the certificate with _id exists
    Revoke certificate by setting revoked status to true and emit certificateRevoked event
```

2. Contract Institution

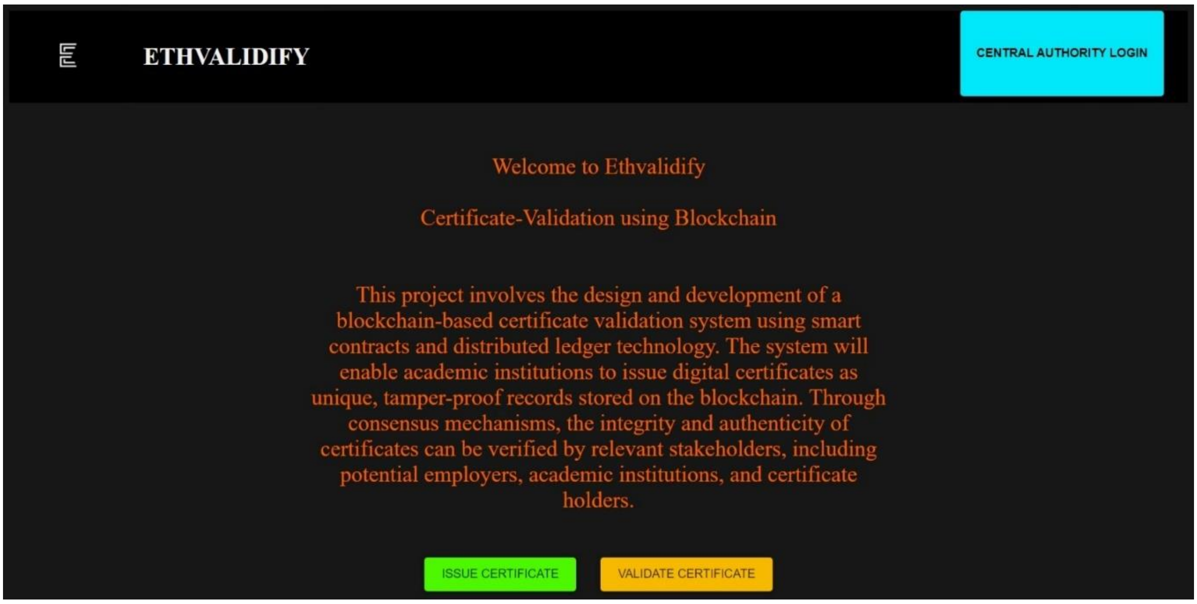
```
State Variables:
    owner: address
    institutes: mapping(address => Institute)
    instituteCourses: mapping(address => Course[])

Events:
    instituteAdded(string _instituteName)

Constructor:
    Institution()
        owner = msg.sender

Struct Course:
    course_name: string
    // Other attributes can be added

Struct Institute:
    institute_name: string
    institute_acronym: string
    institute_link: string

Function stringToBytes32:
    Convert string to bytes32

Function addInstitute:
    Inputs: address _address, string _institute_name, string _institute_acronym, string _institute_link, Course[] _institute_courses
    Only owner can add institute
    Check if institute already exists
    Validate at least one course is added
    Create institute and add courses

Function getInstituteData:
    (Called by Institutions)
    Returns: string, string, string, Course[]
    Retrieve institute data for the calling address

Function getInstituteData (Overloaded):
    (Called by Smart Contracts)
    Inputs: address _address
    Validate smart contract ownership
    Retrieve institute data for the provided address

Function checkInstitutePermission:
    Inputs: address _address
    Returns: bool
    Check if an institute exists for the provided address
```

3. Admin

```
Import necessary dependencies and components

Define styles using withStyles and create Material-UI components

Create the Admin class component
  Set initial state variables

  Define lifecycle method componentWillMount()
    - Call methods to load Web3 MetaMask and Blockchain data

  Define method loadWeb3Metamask()
    - Check if MetaMask is available, set up Web3

  Define method loadBlockChainDataAndCheckAdmin()
    - Fetch Ethereum accounts and network details
    - Check if the connected account is the owner of the smart contract
    - Update state variables based on conditions

  Define other helper methods for handling form changes, adding institutes, course handling, dialogs, etc.

  Render method:
    - Conditionally render loading states, admin views, or error messages based on state variables

Export the component with styles applied
```

APPENDIX-B

SCREENSHOTS

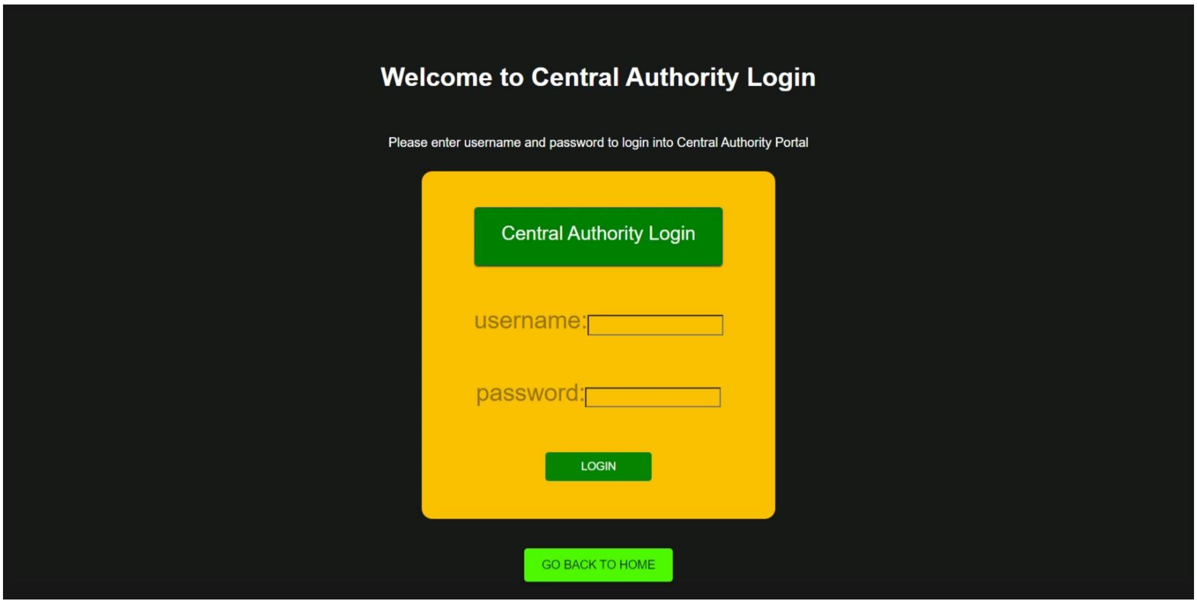


Welcome to Ethvalidify

Certificate-Validation using Blockchain

This project involves the design and development of a blockchain-based certificate validation system using smart contracts and distributed ledger technology. The system will enable academic institutions to issue digital certificates as unique, tamper-proof records stored on the blockchain. Through consensus mechanisms, the integrity and authenticity of certificates can be verified by relevant stakeholders, including potential employers, academic institutions, and certificate holders.

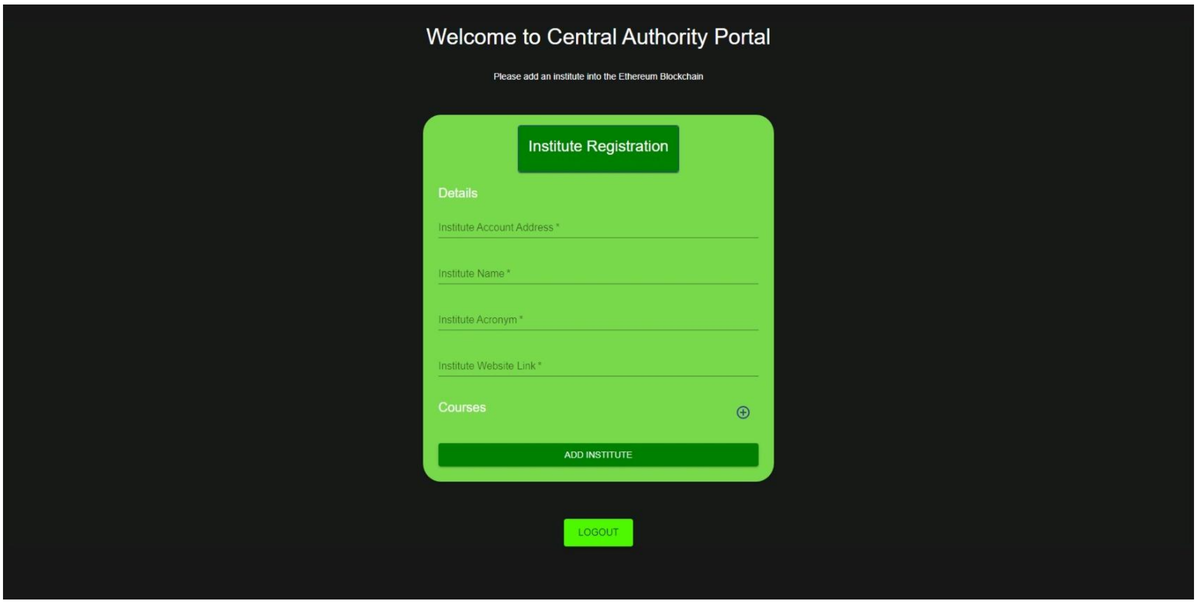
Figure B.1 – Homepage of Ethvalidify



Welcome to Central Authority Login

Please enter username and password to login into Central Authority Portal

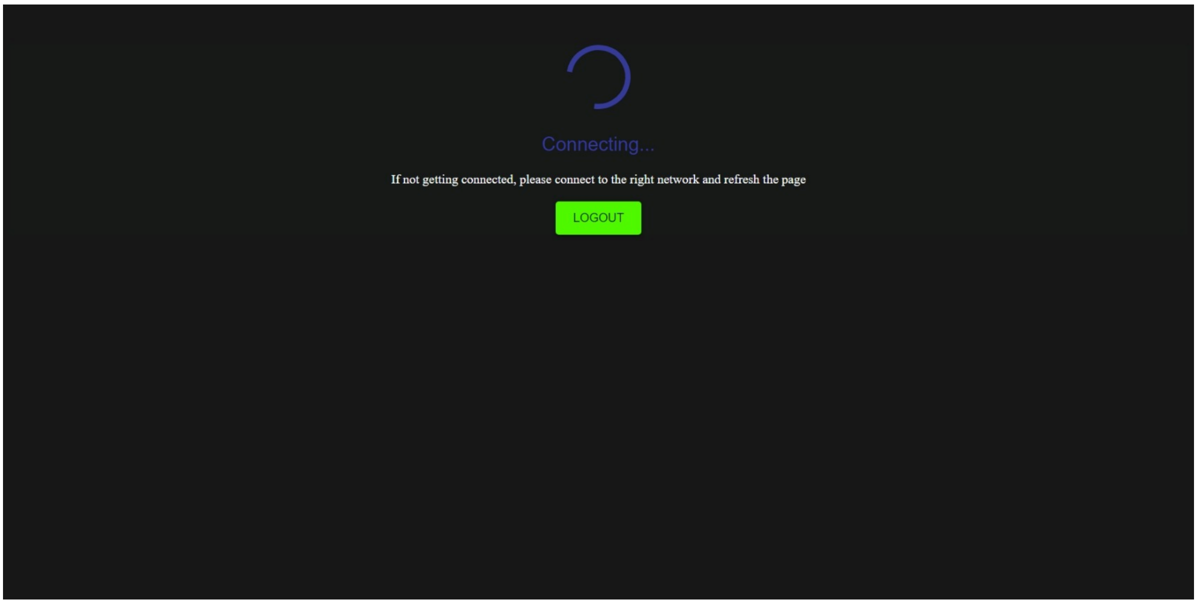
Figure B.2 – Login Page



Welcome to Central Authority Portal

Please add an institute into the Ethereum Blockchain

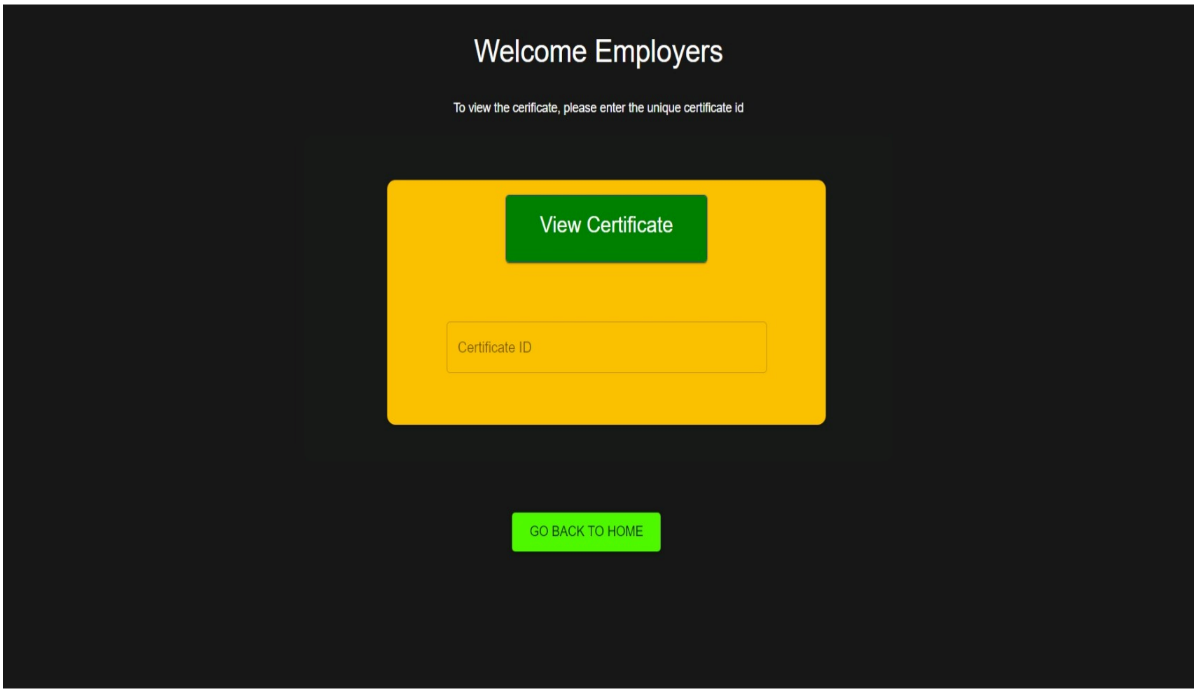
Figure B.3 – Central Authority Portal



Connecting...

If not getting connected, please connect to the right network and refresh the page

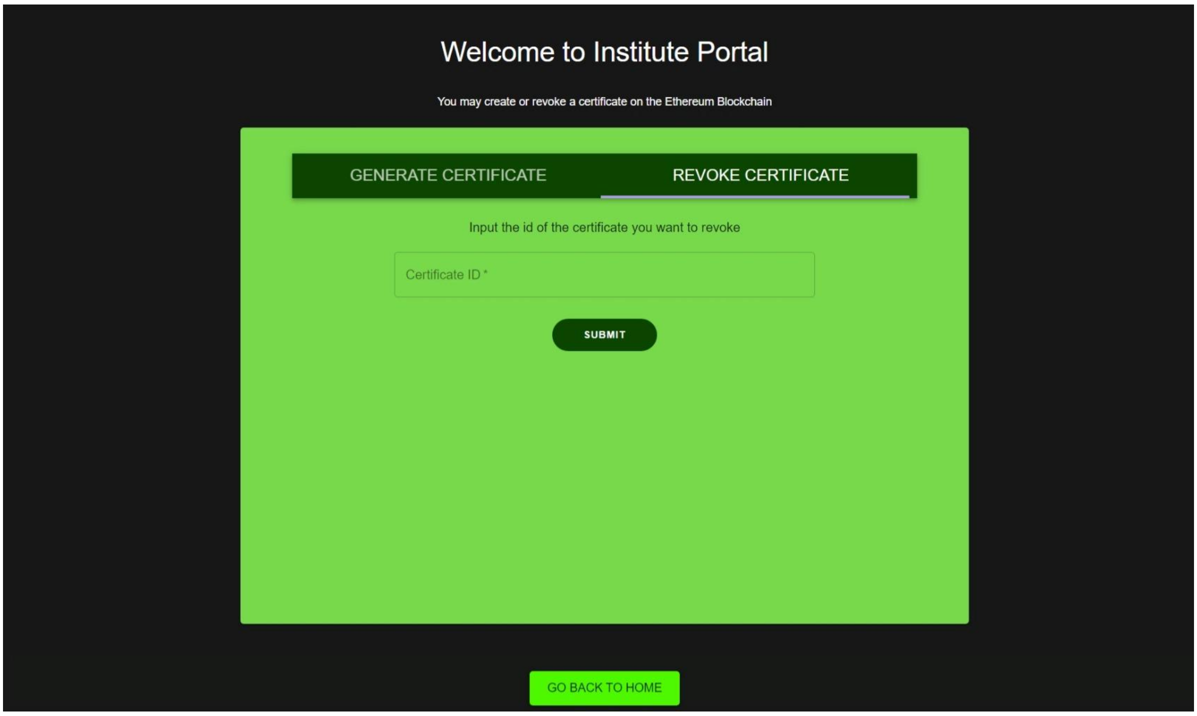
Figure B.4 – Loading page



Welcome Employers

To view the cerficate, please enter the unique certificate id

Figure B.5 – Employers Portal

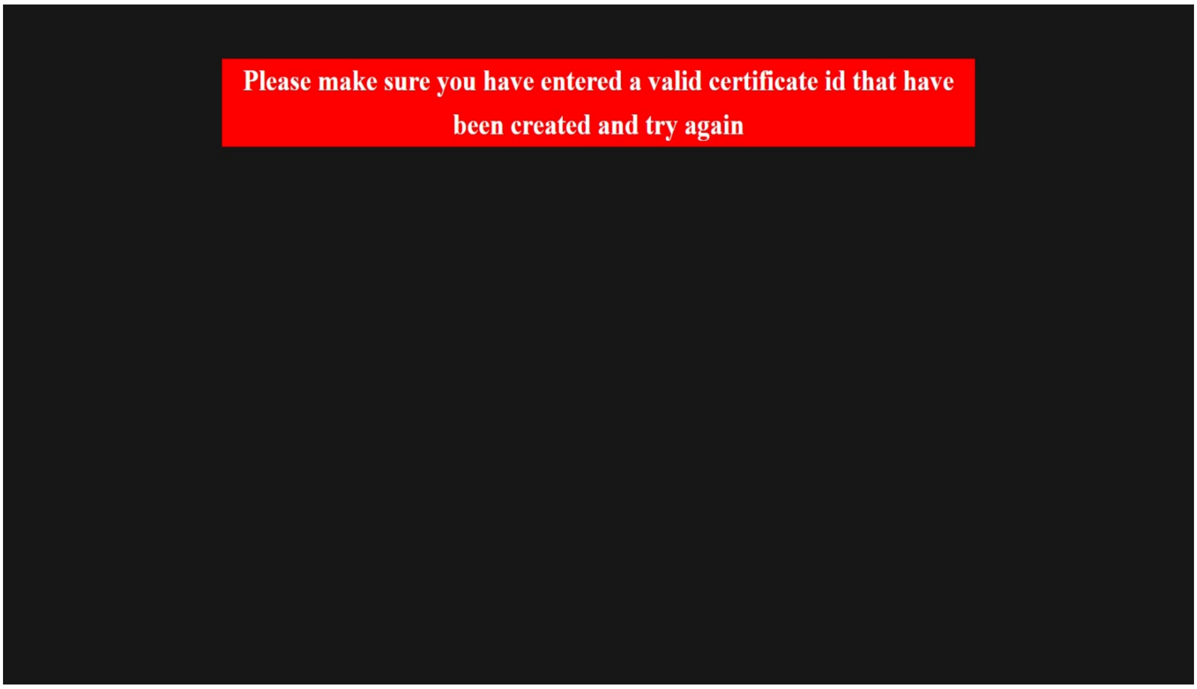


Welcome to Institute Portal

You may create or revoke a certificate on the Ethereum Blockchain

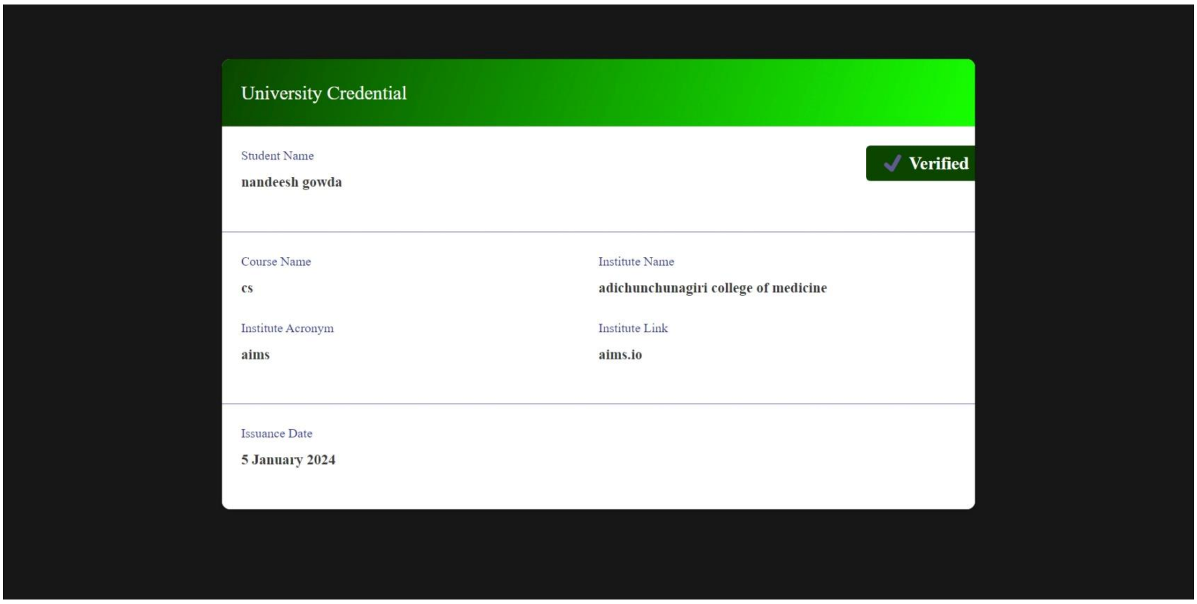
Input the id of the certificate you want to revoke

Figure B.6 – Institute Portal(Revoke form)



Please make sure you have entered a valid certificate id that have been created and try again

Figure B.7 – Error Message Display



University Credential

Student Name
nandeesh gowda

✓ Verified

Course Name
cs

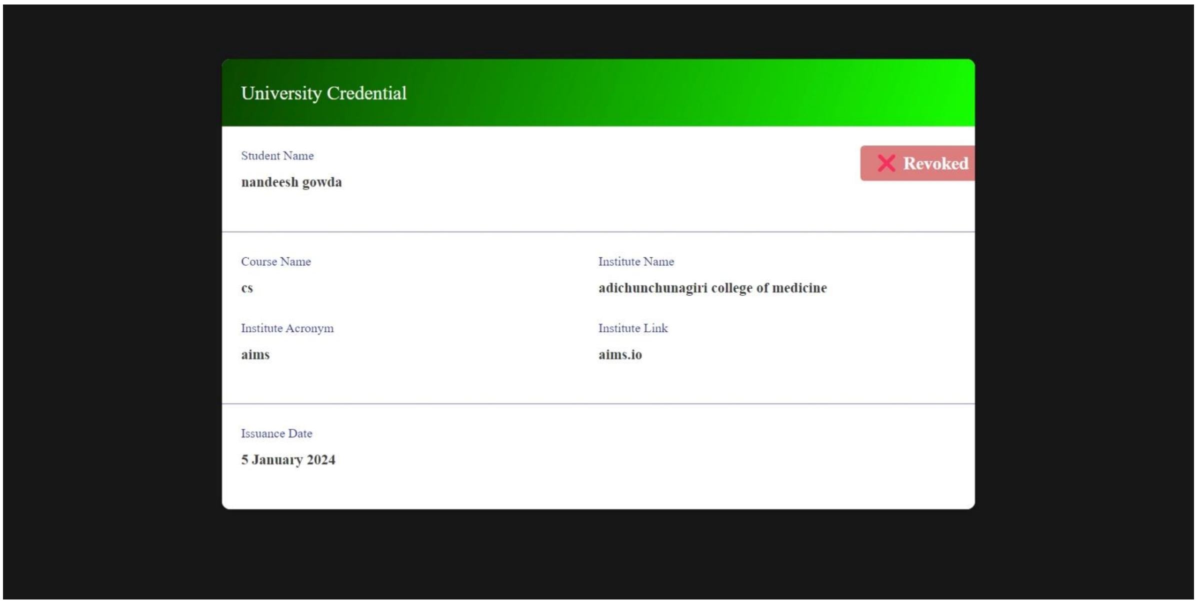
Institute Name
adichunchunagiri college of medicine

Institute Acronym
aims

Institute Link
aims.io

Issuance Date
5 January 2024

Figure B.8 – Generated Certificate



University Credential

Student Name
nandeesh gowda

✕ Revoked

Course Name
cs

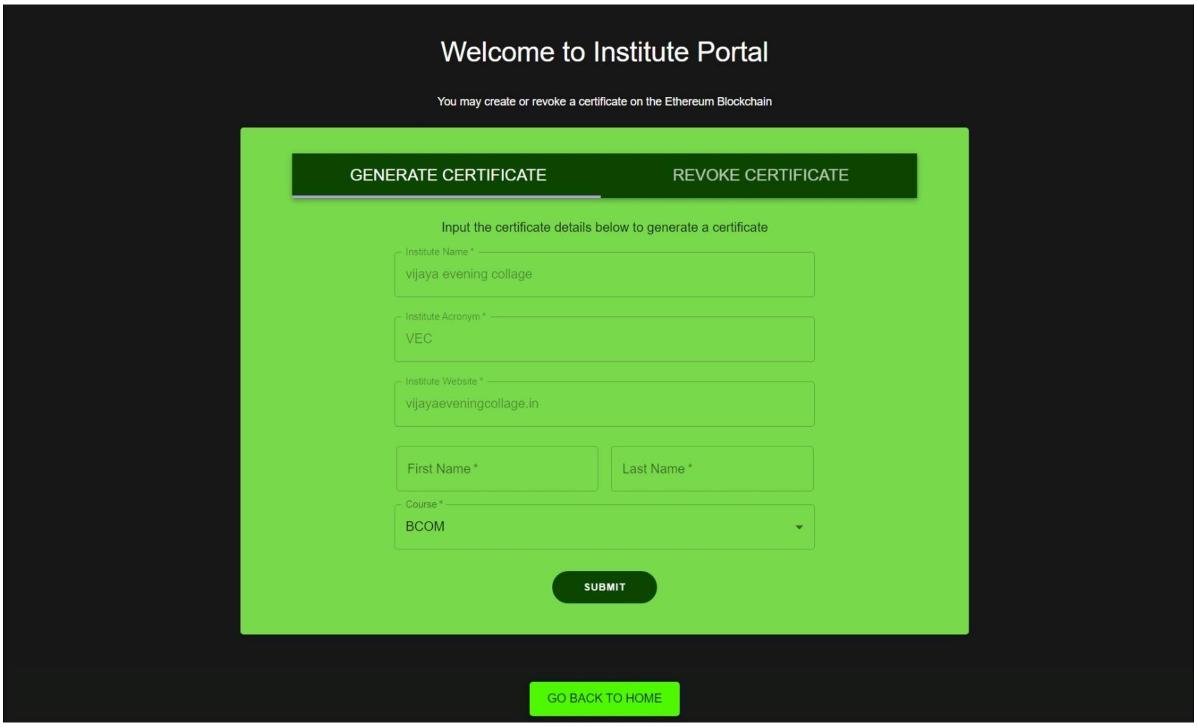
Institute Name
adichunchunagiri college of medicine

Institute Acronym
aims

Institute Link
aims.io

Issuance Date
5 January 2024

Figure B.9 – Revoked Certificate



Welcome to Institute Portal

You may create or revoke a certificate on the Ethereum Blockchain

Input the certificate details below to generate a certificate

Institute Name * vijaya evening collage

Institute Acronym * VEC

Institute Website * vijayaeveningcollage.in

First Name *

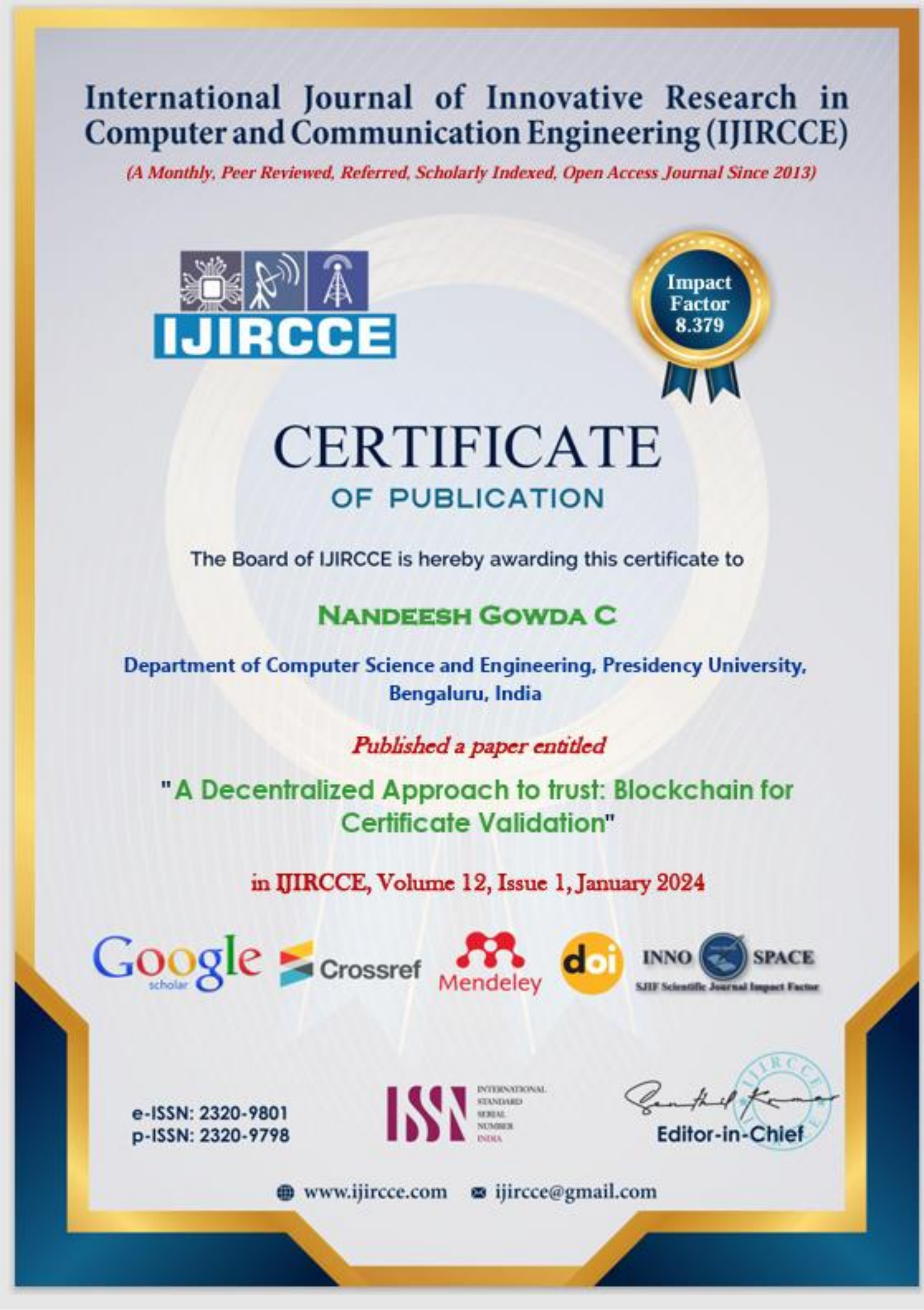
Last Name *

Course * BCOM

Figure B.10 – Institute Portal(Generate Certificate form)

APPENDIX-C

ENCLOSURES



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Referred, Scholarly Indexed, Open Access Journal Since 2013)

IJIRCCE

Impact Factor 8.379

CERTIFICATE

OF PUBLICATION

The Board of IJIRCCE is hereby awarding this certificate to

NANDEESH GOWDA C

Department of Computer Science and Engineering, Presidency University, Bengaluru, India

Published a paper entitled

"A Decentralized Approach to trust: Blockchain for Certificate Validation"

in IJIRCCE, Volume 12, Issue 1, January 2024

Google scholar Crossref Mendeley doi INNO SPACE SJIF Scientific Journal Impact Factor

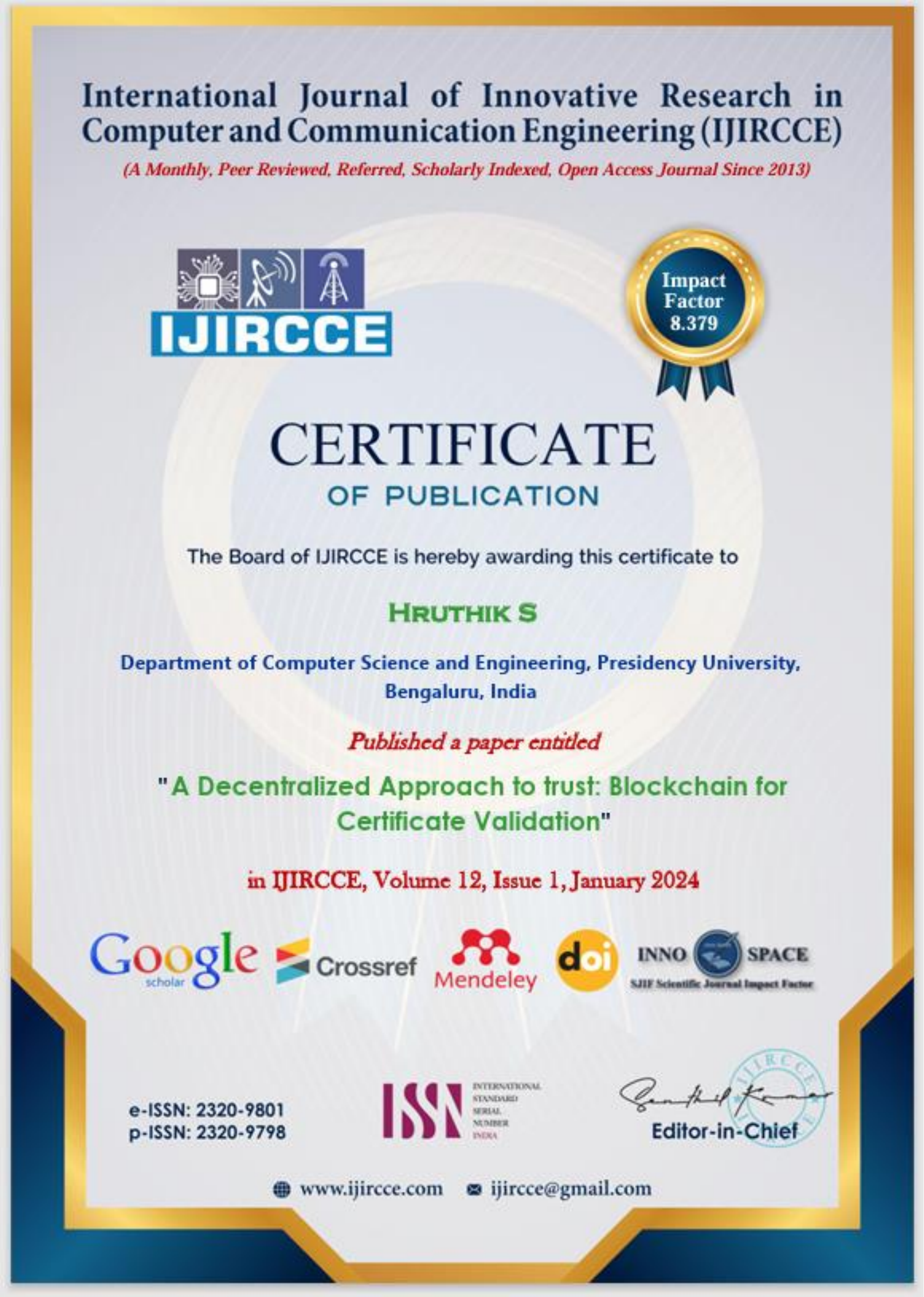
e-ISSN: 2320-9801
p-ISSN: 2320-9798

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Editor-in-Chief

www.ijircce.com ijircce@gmail.com

Figure C.1 – Certificate of Publication



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Referred, Scholarly Indexed, Open Access Journal Since 2013)

IJIRCCE

Impact Factor 8.379

CERTIFICATE

OF PUBLICATION

The Board of IJIRCCE is hereby awarding this certificate to

HRUTHIK S

Department of Computer Science and Engineering, Presidency University, Bengaluru, India

Published a paper entitled

"A Decentralized Approach to trust: Blockchain for Certificate Validation"

in IJIRCCE, Volume 12, Issue 1, January 2024

Google scholar Crossref Mendeley doi INNO SPACE SJIF Scientific Journal Impact Factor

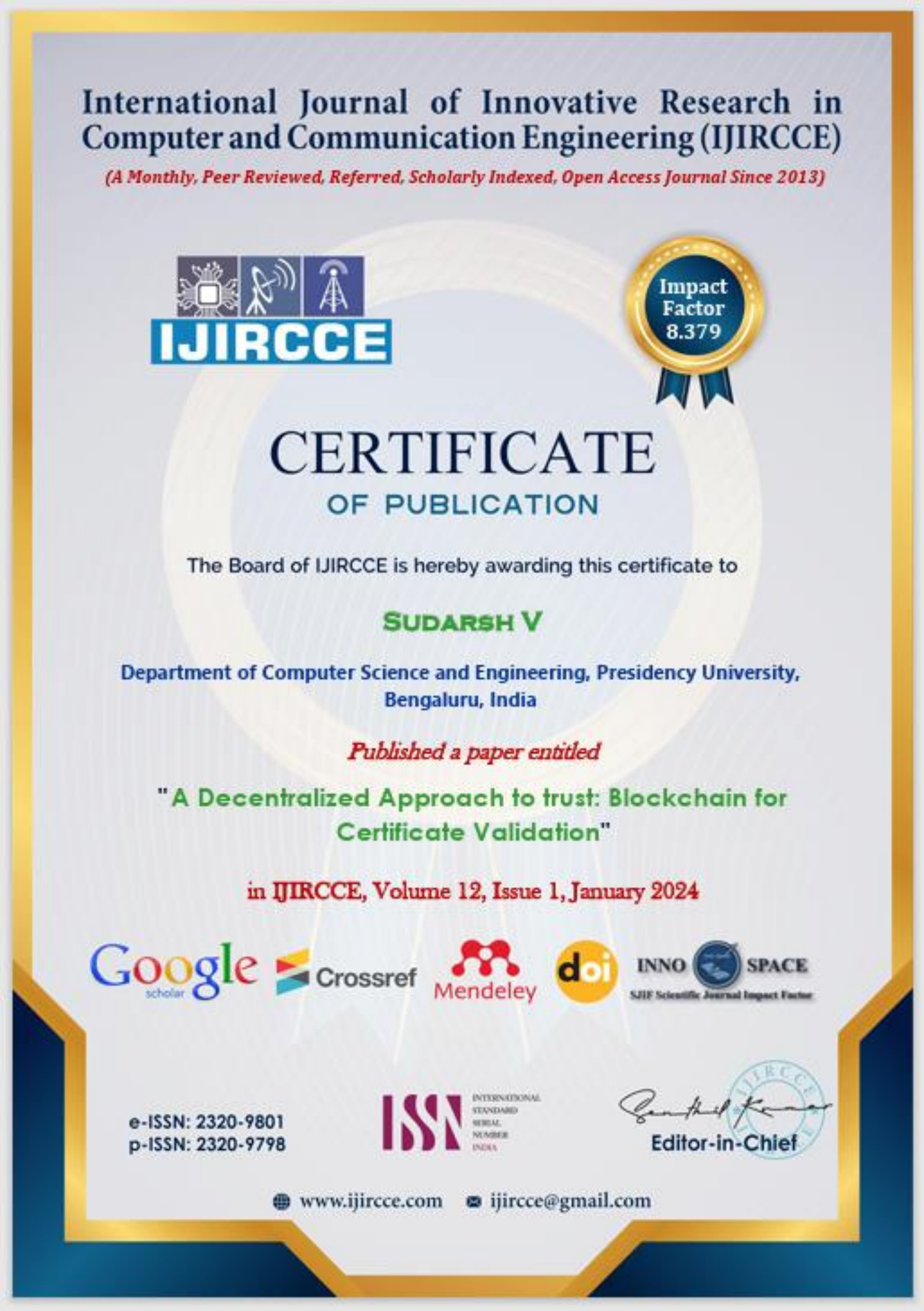
e-ISSN: 2320-9801
p-ISSN: 2320-9798

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Editor-in-Chief

www.ijircce.com ijircce@gmail.com

Figure C.2 – Certificate of Publication



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Referred, Scholarly Indexed, Open Access Journal Since 2013)

IJIRCCE

Impact Factor 8.379

CERTIFICATE

OF PUBLICATION

The Board of IJIRCCE is hereby awarding this certificate to

SUDARSH V

Department of Computer Science and Engineering, Presidency University, Bengaluru, India

Published a paper entitled

"A Decentralized Approach to trust: Blockchain for Certificate Validation"

in IJIRCCE, Volume 12, Issue 1, January 2024

Google scholar Crossref Mendeley doi INNO SPACE SJIF Scientific Journal Impact Factor

e-ISSN: 2320-9801
p-ISSN: 2320-9798

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

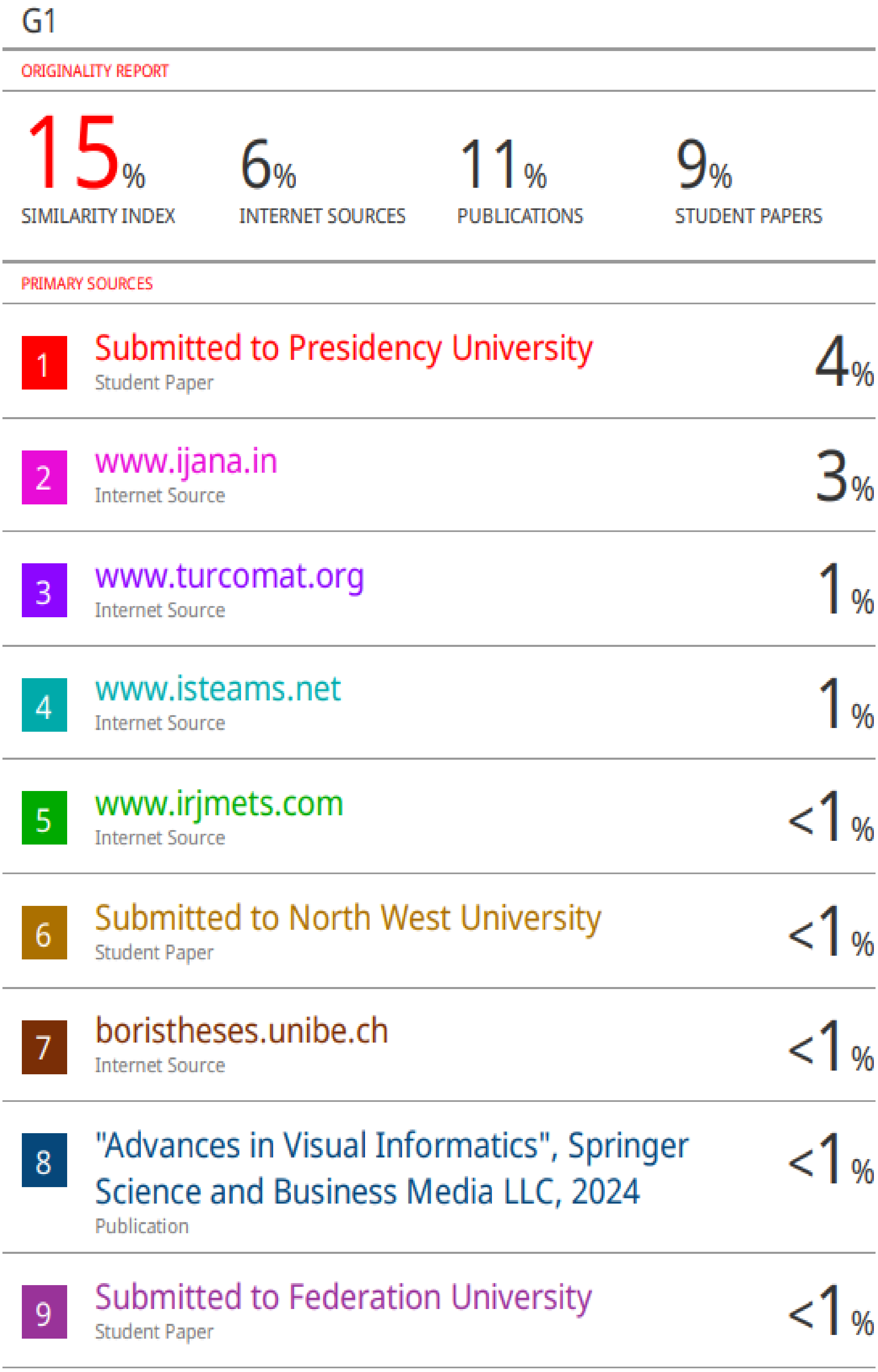
Editor-in-Chief

IJIRCCE

www.ijircce.com ijircce@gmail.com

Figure C.3 – Certificate of Publication

Plagiarism Report



G1

ORIGINALITY REPORT

15%	6%	11%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Presidency University Student Paper	4%
2	www.ijana.in Internet Source	3%
3	www.turcomat.org Internet Source	1%
4	www.isteams.net Internet Source	1%
5	www.irjmets.com Internet Source	<1%
6	Submitted to North West University Student Paper	<1%
7	boristheses.unibe.ch Internet Source	<1%
8	"Advances in Visual Informatics", Springer Science and Business Media LLC, 2024 Publication	<1%
9	Submitted to Federation University Student Paper	<1%

Sustainable Development Goals

SUSTAINABLE DEVELOPMENT GOALS
17 GOALS TO TRANSFORM OUR WORLD
1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
SUSTAINABLE DEVELOPMENT GOALS

The Project work carried out here is mapped to SDG-9 Industry, Innovation and Infrastructure.

This project aligns with SDG-9, Industry, Innovation, and Infrastructure, by fostering technological innovation and enhancing infrastructure development. Through its initiatives, the project contributes to building resilient, inclusive, and sustainable industrialization, promoting innovation, and ensuring access to reliable, sustainable, and modern infrastructure, thus advancing the objectives of SDG-9.