CERTIQ – A DECENTRALIZED CERTIFICATE ISSUANCE AND VERIFICATION SYSTEM

A MINI PROJECT REPORT

submitted by

ADITHYAN MARIKKAL	**NSS22CS009**
KEERTHANA S	**NSS22CS037**
NIYALURAHMAN K K	**NSS22CS049**
AMEYA SHYJU M	**LNSS22CS069**

to

The APJ Abdul Kalam Technological University

in partial fulfillment of the requirements for the award of the Degree

of

Bachelor of Technology

in

Computer Science and Engineering

Department of Computer Science and Engineering

NSSCE Palakkad

APRIL 2025

DECLARATION

We undersigned hereby declare that the project report **CertiQ - A Decentralized Certificate Issuance and Verification** submitted for partial fulfillment of the requirements for the award of the degree of Bachelor of Technology of the APJ Abdul Kalam Technological University, Kerala, is a bonafide work done by us under supervision of **MAANASA N A S**. This submission incorporates ideas from various sources, and we have adequately and accurately cited and referenced the original sources. We also declare that we have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in my submission. We understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not previously formed the basis for the award of any degree, diploma or similar title of any other University.

ADITHYAN MARIKKAL
KEERTHANA S
NIYALURAHMAN K K
AMEYA SHYJU M

Place: Palakkad
Date: 29-04-2025

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NSSCE Palakkad

PALAKKAD

APRIL 2025

CERTIFICATE

This is to certify that the report entitled **CertiQ - A Decentralized Certificate Issuance and Verification** submitted by **ADITHYAN MARIKKAL, KEERTHANA S, NIYALURAHMAN K K, AMEYA SHYJU M** to the APJ Abdul Kalam Technological University in partial fulfillment of the requirements for the award of the Degree of Bachelor of Technology in Computer Science and Engineering is a bonafide record of the project work carried out by him/her under my/our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

Internal Supervisor	Project Coordinator
Name : Prof. Guide Name	Name : Prof. Coordinator 2
Signature :	Signature : .....
Project Coordinator	Head of Department
Name : Prof. Coordinator 1	Name : Prof. HoD Name
Signature :	Signature : .....

ACKNOWLEDGMENT

First and foremost, we are grateful to God for blessing us with the strength, knowledge,and determination to undertake this project. We would like to extend our heartfelt thanks to principal **Dr.Rajeev N**, for providing us the opportunity to do this project. We are also grateful to **Dr. Viji Rajendran V**, Professor, Head of the Department of Computer Science and Engineering, for the constant support and encouragement throughout the project. We would like to express our sincere appreciation to our project guide,Asst. Professor Maanasa N A S, for her invaluable guidance, expertise and patience whose suggestions shaped this project and enhanced the quality. We are indebted to all teaching and non- teaching staff of the Department of Computer Science and Engineering for their constant support, valuable inputs and assistance. Lastly, we would like to extend our heartfelt thanks to all our friends and well-wishers who provided us with moral support, encouragement and motivation throughout this project. And to our beloved parents, we owe a special debt of gratitude. Their love, encouragement and belief have always been a source of motivation for us.

ADITHYAN MARIKKAL

KEERTHANA S

NIYALURAHMAN K K

AMEYA SHYJU M

Place: Palakkad

Date: 29-04-2025

ABSTRACT

The growing reliance on digital certificates for secure communication and authentication faces challenges like tampering, inefficiency, and centralized authority risks. CertiQ addresses these issues by leveraging blockchain technology and cryptographic techniques to create a decentralized, tamperproof system for certificate issuance, storage, validation, and revocation. The platform automates certificate lifecycle management, enhances security, and enables the seamless revocation of invalid or compromised certificates, reducing reliance on central authorities. By utilizing blockchain's immutability and cryptographic protocols, CertiQ aims to provide a seamless and secure platform for managing certificates across applications such as secure web communications, API integrations, and blockchain-based trust systems. The expected outcomes include enhanced certificate security, reduced dependency on centralized entities, and improved trust in digital transactions. Keywords: digital certificates, blockchain, cryptographic security, decentralized systems, certificate revocation.

CONTENTS

LIST OF FIGURES

Chapter 1

INTRODUCTION

1.1 CERTIFICATE MANAGEMENT SYSTEM

In today's fast changing digital world, the need for secure and tamper-proof records has become more significant than ever. Traditional certificate issuance and verification methods relying on paper or centralized databases are prone to fraud, forgery, and data breaches. This project aims to address these challenges by developing an innovative blockchain-based certificate issuance and verification system.

Our system leverages the inherent security and immutability of blockchain technology to create a decentralized platform for managing academic, professional, and other credentials. By utilizing blockchain's distributed ledger, we aim to enhance the authenticity, integrity, and security of certificates while streamlining the issuance, verification and revocation processes for both issuers and verifiers.

1.2 BLOCKCHAIN TECHNOLOGY

The Blockchain is a distributed database of records of all transactions or digital events across a decentralized network of computers. Each transaction is verified by a majority of participants of the system. There is no central server or system which keeps the data of the Blockchain. This system allows the Notarization of Data as it is present on every Node and is publicly verifiable. The immutable and transparent nature of blockchain ensures that records are secure, trustworthy, resistant to tampering.

Chapter 2

PROBLEM STATEMENT

Verification of certificates remains a significant challenge due to the risks of forgery, data manipulation, and reliance on centralized authorities. Traditional methods, either paper-based or digital, suffer from inefficiencies, security vulnerabilities, and lack of transparency. Centralized databases are prone to security breaches, unauthorized modifications, and single points of failure, making the verification process slow, costly, and unreliable. Issuers face administrative burdens, high costs, and the risk of counterfeit certificates that undermine their credibility. Verifiers face time-consuming and inefficient validation processes, delaying employment and educational enrollments, while certificate holders often deal with lost, damaged, or inaccessible records, leading to frustration and missed opportunities. These limitations highlight the urgent need for a secure, decentralized, and transparent certification management system to ensure trust, efficiency, and accessibility for all stakeholders.

2.1 SCOPE

The project focuses on the design, development, and deployment of a decentralized digital certificate management system that uses polygon blockchain and IPFS. It enables the creation, issuance, revocation, and verification of digital certificates through smart contracts, ensuring transparency and security. To enhance efficiency, only minimal certificate metadata is stored on-chain, while the actual certificate files are securely distributed via IPFS. The system supports multiple user

roles, allowing authorized institutions to register as issuers and manage certificates, recipients to access and share their credentials, and verifiers to authenticate certificate legitimacy. Using Polygon's scalable and Ethereum-compatible infrastructure, CertiQ ensures an efficient, secure, and decentralized approach to digital credential management.

2.2 OBJECTIVES

The objective is to create a decentralized, secure, and transparent system to issue, manage, and verify digital certificates, ensuring authenticity, efficiency, and ease of access for both issuers and verifiers. Key features include tamper proof certification, automated verification, reduced administrative overhead, a user-friendly interface for seamless adoption, and the ability of institutions to revoke certificates when necessary. This is achieved using blockchain for immutability, smart contracts for automation, and IPFS for distributed storage, eliminating reliance on centralized authorities while improving trust and security.

2.3 FEASIBILITY

1. Blockchain Technology:
- EVM Compatibility: Polygon ensures seamless integration with Ethereum's ecosystem, enabling the use of Solidity for smart contracts and existing development tools.
2. Polygon Network:
- Layer-2 Scaling: Polygon's low fees and high speeds ensure cost-effective and efficient operations.
- Test Network: Polygon's test networks facilitate thorough development and testing before deployment.

3. IPFS for Decentralized Storage:

- Proven Technology: IPFS offers reliable decentralized storage with cryptographic data verification.

- Integration: Easy integration via JavaScript libraries reduces development time and effort.

4. Frontend and Backend Technologies:

- Web Frameworks: React.js (frontend) and Node.js (backend) ensure rapid development, extensive resources, and strong community support.

- Wallet Libraries: Ethers.js enables secure wallet connections and transactions.

Chapter 3

PROPOSED SYSTEM DESIGN

3.1 SYSTEM ARCHITECTURE

The system consists of the following components:

3.1.1 FRONTEND

User Interface : The user interface allows institutes to register and log in using MetaMask-based authentication. Authorized institutes can issue certificates that come with a unique ID. A verification portal is provided where the credentials in the certificates can be displayed and verified using the certificate ID.

3.1.2 BACKEND (Blockchain & Database)

The system integrates smart contracts and blockchain technology to ensure secure and transparent certificate issuance. Certificates are stored on the blockchain as immutable records, with each one assigned a unique hash to prevent duplication. Decentralized storage ensures security and transparency without relying on centralized databases. A revocation mechanism is in place, allowing only the issuing institutes to revoke certificates, which updates the blockchain status accordingly. For verification and security, users can verify certificates using the unique ID without the need for wallet authentication. The certificates are stored permanently on the blockchain, offering tamper-proof storage that prevents forgery.

3.2 CORE FEATURES

Add Institute: The Institution contract owner can register new educational or certification institutions, enabling them to issue certificates through the platform.

Issue Certificate: This feature enables registered institutions to create and issue certificates to individuals who have successfully completed a course or training.

Revoke Certificate: This feature allows registered institutions to invalidate previously issued certificates, typically due to expiration, fraud, or other valid reasons.

Verify Certificate: This feature allows anyone (e.g., employers, educational institutions, other verifiers) to verify the authenticity and validity of a certificate using its unique ID.

3.3 SYSTEM DESIGN

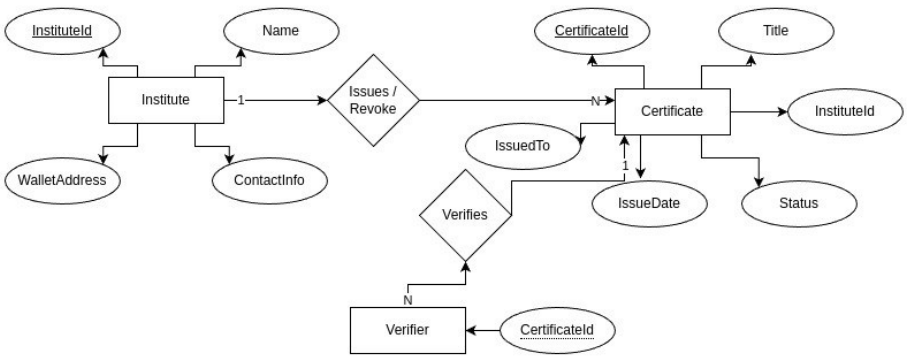

Figure 3.1: ER-Diagram

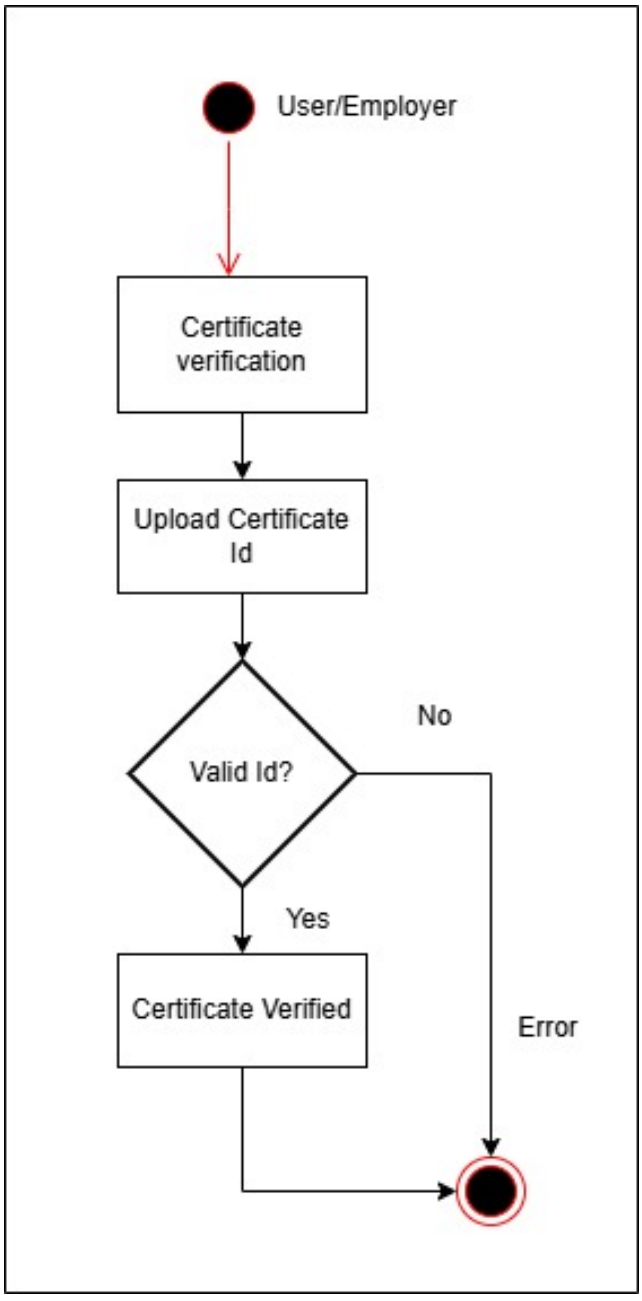

Figure 3.2: Activity Diagram

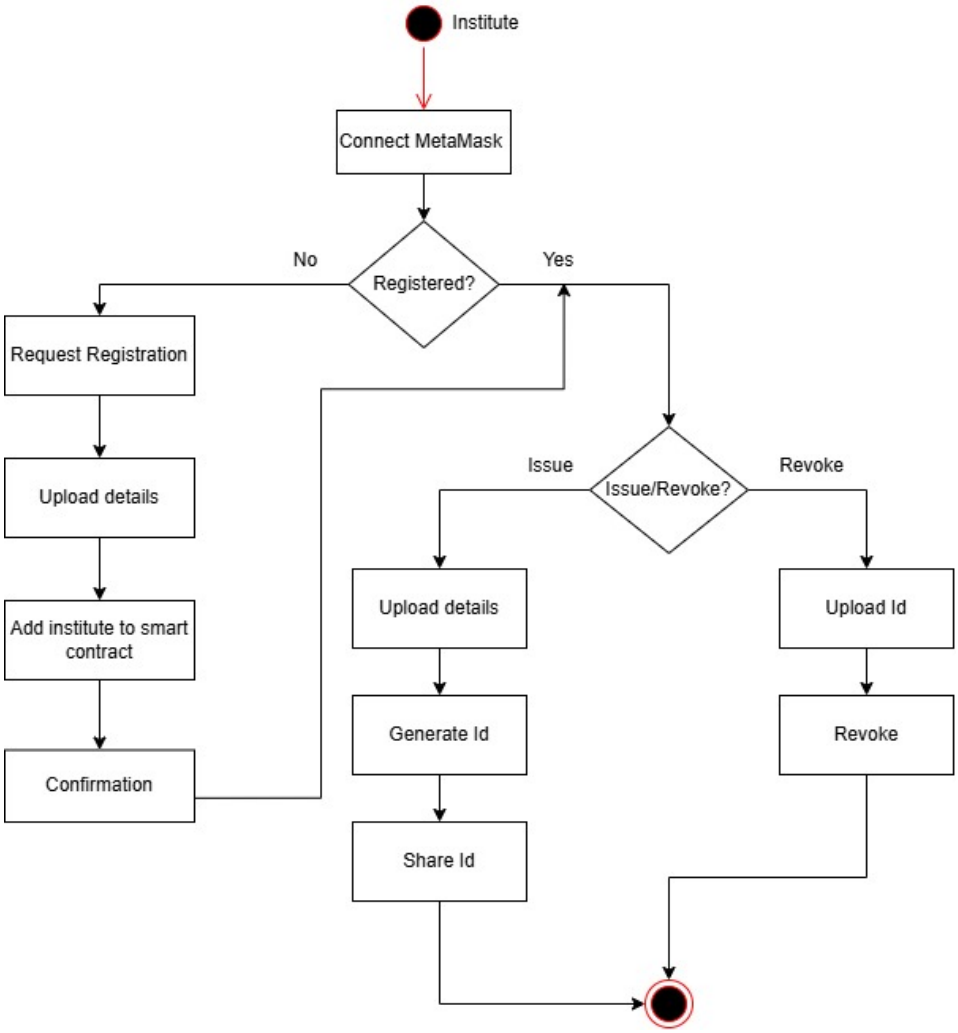

Figure 3.3: Activity Diagram

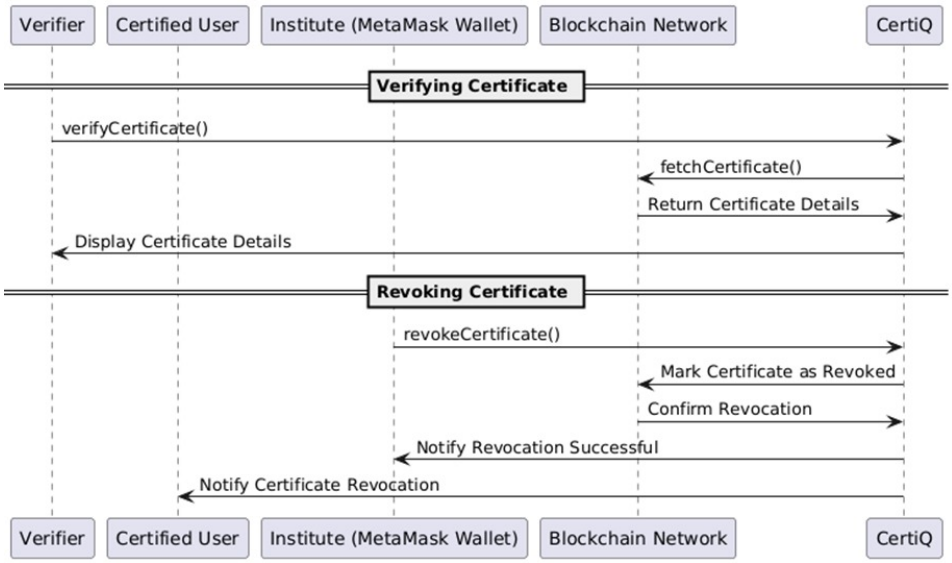

Figure 3.4: sequence

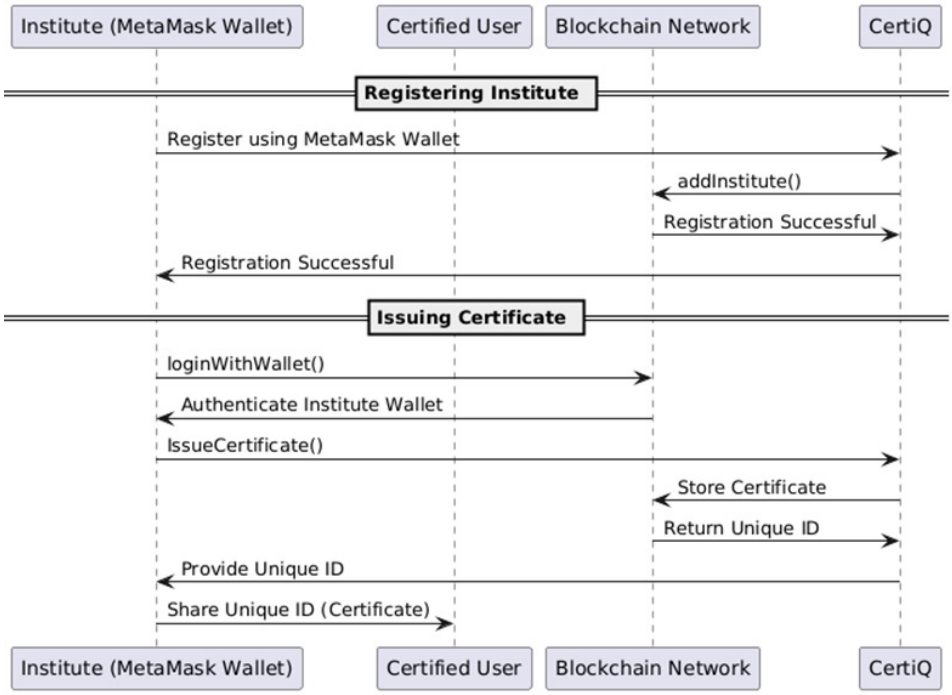

Figure 3.5: sequence

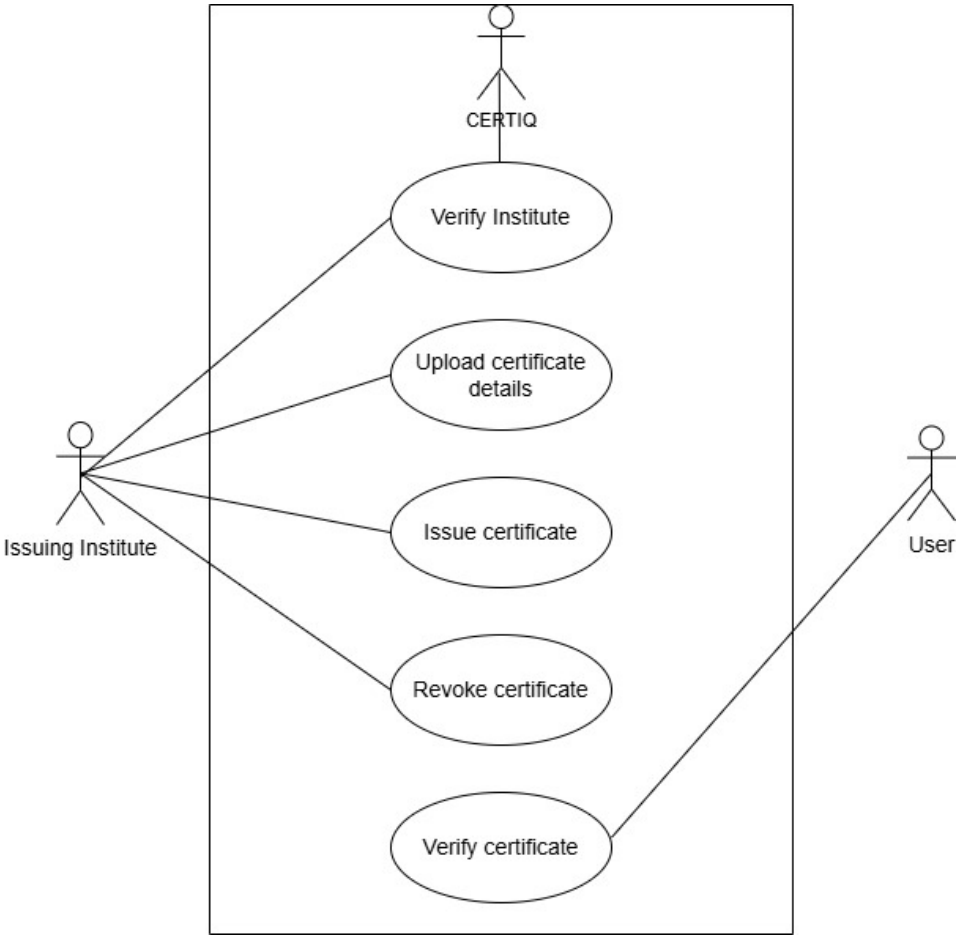

Figure 3.6: usecase

Chapter 4

LITERATURE REVIEW

[1]*Educational Certificate Verification System Using Blockchain.(2020)*The verification of documents submitted by prospective employees by the employer is essential before offering jobs. As the process is manual, it takes an ample amount of time for the candidate to receive an offer letter. The authorities issuing certificates verify the authenticity of the certificates and acknowledge them to the employers. Such a time-consuming verification process delays the hiring process. As a solution to counterfeit academic certificates, a distributed ledger is provided by Blockchain along with the cryptography mechanism. According to [1] the use of Blockchain makes it possible to have a shared platform for warehousing and retrieving certificates, hence minimizing the time required for verifying the certificates.

[2] *Efficient Certificate Management in Blockchain based Internet of Vehicles.(2020)* As the Online of Vehicle (IoV) research trend continues, the privacy and security of each internet automobile has become a hot topic. This study aims to lower the cost of securely certifying documents such as graduation certificates. The distribution and maintenance of the Certificate Revocation List (CRL) in vehicle public key infrastructure are addressed in this article using blockchain technology (PKI). For the blockchain mechanism, the suggested scheme employs activation codes to validate the certificate based on time to non-revoked vehicle. We want to cut the cost of certification and, of course, do rid of the certificates for automobiles that are no longer in use.

[3]*Design and Implementation of Work Training Certificate Verification Based On Public Blockchain Platform.*The goal of this study is to create a public blockchain-based system for storing job training documents. Certificate data is secured using public platforms, making it harder to forge. Smart contracts are used to create data for blocks that will be delivered to the Ethereum blockchain network. The Inter Planetary File System (IPFS) is used to store certificate files in a distributed environment, allowing for quick and secure access. The findings revealed that certificate data can be kept on the Ethereum public blockchain architecture, with supporting files in the IPFS environment. The findings revealed that certificate data can be kept on the Ethereum public blockchain architecture, with supporting files in th IPFS environment.

[4]*Towards Decentralised Cloud Storage with IPFS: Opportunities, Challenges, and Future Considerations* paper provides a detailed analysis of the InterPlanetary File System (IPFS), a decentralized storage architecture that utilizes peer-to-peer networking and content addressing. It highlights the strengths of IPFS, such as its ability to offer secure and tamper-proof data storage through content identifiers (CIDs), and its growing role in decentralized systems. The authors also explore critical challenges, including the lack of built-in access control and the need for effective incentivization to maintain network participation.

[5]*Smart Contract: Security and Privacy* examines the application of smart contracts in modern systems, focusing on their role in enhancing security and privacy. It provides an overview of smart contract mechanics and their applications in industries such as real estate and logistics. The study emphasizes the importance of secure coding practices to prevent vulnerabilities, which is crucial for automating processes like certificate issuance, verification, and revocation. It

also highlights the need for a secure development process and regular security audits to ensure the reliability of smart contracts.

REFERENCES

[1] INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 03, MARCH 2020 ISSN 2277-8616 82 IJSTR©2020 www.ijstr.org Educational Certificate Verification System Using Blockchain Dinesh Kumar K, Senthil P, Manoj Kumar D.S

[2] Efficient Certificate Management in Blockchain based Internet of Vehicles Ei Mon Cho 1, Maharage Nisansala Sevwandi Perera22020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID)

[3] Efficient Certificate Management in Blockchain based Internet of Vehicles Ei Mon Cho 1, Maharage Nisansala Sevwandi Perera22020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID) 1971.

[4] Towards Decentralised Cloud Storage with IPFS: Opportunities, Challenges, and Future Considerations" Trinh Viet Doan (Technical University of Munich), Yiannis Psaras (Protocol Labs), Jörg Ott (Technical University of Munich), Vaibhav Bajpai (CISPA Helmholtz Center for Information Security)

[5] Smart Contract: Security and Privacy Leena S. Alotaibi and Sultan S. Alshamrani (Department of Information Technology, College of Computer and Information Technology, Taif University, Saudi Arabia)