Ethereum-Powered E-Certificate Issuance and Verification

Abstract

Nowadays verification and sharing of academic certificates often involve difficult processes that require time and resources. Institutions and organizations must engage in manual communication to verify credentials which can be inefficient and prone to errors. To address these challenges, this project introduces Ethereum-Powered E-Certificate Issuance and Verification system. This is a blockchain-based system designed to provide secure certificate management system. Using the transparency and immutability of the Ethereum blockchain, the system able to issue tamper-proof digital certificates. That are securely stored and easily accessible. The proposed solution uses Solidity smart contracts to create a decentralized database where certificates are linked to student's digital wallets. This is eliminating the need for intermediaries in the verification process. Once issued, certificates are immutable, ensuring their authenticity and safe guarding against fraud. A user-friendly portal allows third parties, such as employers, to verify certificates instantly by comparing their cryptographic hash with the one stored on the blockchain. This proccess not only improves security but also significantly reduces the administrative burden of credential verification, offering a scalable, transparent and efficient alternative of traditional methods.This system redefines certificate management by ensuring that individuals can share and verify their credentials effortlessly. It is fostering trust and reliability across academic and professional landscapes.

Keywords: Blockchain, Smart contract, E-certificate, Metamask.

Acknowledgements

I want to start by thanking my supervisor Ishtiaque Zahid. He gives me valuable time by giving me important resources and guiding me in achieving my project's primary goal. I appreciate his active counsel in helping me to choose the best approaches to overcome obstacles.

Lastly, I want to show my appreciation to the Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet 3114, Bangladesh, for their beneficial assistance.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Academic certificates are crucial in validating a studentâs achievements, qualifications and skills. They serve as proof of educational background for students. It establish credibility for uni versities and assist employers and other organizations in assessing an individualâs qualifications. Despite their significance, the current system for managing certificates is outdated and fraught with inefficiencies. Traditionally, certificates are issued as physical documents or PDFs. This proccess pose challenges in terms of security, accessibility and long-term usability. In the conventional system, students often encounter difficulties managing multiple certificates over time. Particularly face problem when applying for further education, employment, or professional licensing. Universities face challenges in ensuring that the certificates they issue are secure against forgery or alteration. Third parties such as employers or other institutions frequently need to manually verify certificates. This process is both time-consuming and error-prone. These issues underscore the need for a more efficient solution that enhances security and improves accessibility and verification. Blockchain technology offers a transformative opportunity to modernize this process, with its decentralized and immutable nature. Blockchain can securely store certificates, ensuring they cannot be tampered. It also facilitates verification by third parties without the need for intermediaries. This project proposes a blockchain-based system to address the inefficiencies of traditional certificate management system. it is enabling universities to issue, students to manage and third parties to verify certificates securely and efficiently.

1.1 Problem Definition

The traditional methods of issuing and managing academic certificates present several signifi cant drawbacks, rendering the system inefficient and unreliable. These challenges include:

- **Risk of Fraud**: Physical certificates and digital PDFs are susceptible to forgery. Counter feit certificates pose a growing concern in academia and professional industries, leading to trust issues and complications for employers and institutions.
- **Loss or Damage**: Paper certificates can be easily lost or damaged over time. Even digital certificates stored on personal devices can be accidentally deleted or become inaccessible, leaving individuals without proof of their credentials when needed most.
- **Inefficient Verification**: The verification process for traditional certificates often requires third parties, such as employers, to manually contact the issuing university or institution. This process is not only time-consuming but also resource-intensive for all parties involved.
- **Limited Accessibility and Sharing**:Students often need to physically mail or manually send their certificates to third parties. Sharing certificates across borders or with multiple parties can be slow and inefficient, hindering students and professionals from effectively leveraging their achievements.
- **Lack of Transparency**: Current systems do not provide a transparent method for third parties to instantly confirm the authenticity of certificates, leading to delays and confusion in recruitment, admissions, and other processes.

These issues highlight the need for a modernized system that eliminates the inefficiencies and vulnerabilities of traditional certificate management.

1.2 Motivation

The increasing reliance on technology in education and professional sectors has created an urgent need to modernize certificate management. Certificates are a fundamental part of an individualâs academic and professional journey, yet the existing system fails to address critical concerns such as security, ease of access, and transparency.

Blockchain technology offers a revolutionary solution to these problems. Unlike traditional systems, blockchain ensures that once a certificate is issued, it is securely recorded and cannot be tampered with. This immutability builds trust in the system and eliminates the risks of forgery or unauthorized changes. Additionally, the decentralized nature of blockchain allows certificates to be easily accessible from anywhere in the world, enabling seamless interaction for students and employers.

The motivation for this project arises from a desire to address the challenges faced by students, universities, and third parties:

- **For Universities**: A blockchain-based system allows universities to issue certificates se curely, ensuring they are verifiable and resistant to tampering.
- **For Students**: Blockchain empowers students with full ownership and control over their certificates, allowing them to easily access, manage, and share their credentials without fear of loss.
- **For Verifiers**: Employers and other third parties can instantly verify the authenticity of a certificate using a QR code or unique link, reducing delays and manual effort

This project aims to create a system that is not only technologically advanced but also user friendly, bridging the gap between traditional and modern certificate management. The ultimate goal is to empower all stakeholders by providing a system that is secure, efficient, and transparent

1.3 Objectives

This project aims to develop a blockchain-based certificate management system that addresses the shortcomings of traditional methods while leveraging the strengths of modern technology. The specific objectives are as follows:

- **Secure Certificate Issuance**: Enable universities to issue certificates directly on the blockchain, ensuring they are tamper-proof and securely linked to the respective student.
- **Student Empowerment**: Provide students with a digital wallet to securely store, access, and manage their certificates, granting them full ownership and control over their credentials.

- **Easy Certificate Sharing**: Allow students to share their certificates easily through QR codes or unique links, ensuring efficient presentation of credentials to potential employers, academic institutions, or licensing bodies.
- **Instant and Public Verification**: Enable third parties to verify the authenticity of certificates instantly, without requiring sign-ups or complex processes, through straightforward access via a QR code or link.
- **Efficiency and Transparency**: Streamline the certificate management process, reducing delays and eliminating manual verification tasks for universities and third parties, while providing a transparent process that enhances trust among stakeholders.
- **Seamless User Experience**: Ensure that all stakeholders universities, students, and verifiersâcan interact with the system easily through a user-friendly interface that integrates blockchain technology seamlessly.

Chapter 2

Background Study

2.1 Blockchain Technology

Blockchain is a distributed and decentralized ledger that stores data across multiple nodes in a secure and immutable manner. The key characteristic of blockchain is its ability to ensure that once data is recorded, it cannot be altered or tampered with, providing unparalleled integrity and trust. This feature makes blockchain a revolutionary technology in fields requiring high levels of transparency and security, such as financial systems, healthcare, and education [1, 2].

Blockchain operates on the principle of a shared ledger, where each transaction is verified by a consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS). These mechanisms ensure that all nodes in the network agree on the validity of transactions, eliminating the need for a central authority [2].

2.2 Smart Contracts

Smart contracts are self-executing contracts where the terms of the agreement are directly written into code. These contracts automatically enforce rules and execute transactions when predetermined conditions are met, making them an essential component of blockchain applications. In the context of this project, smart contracts will automate the issuance and verification of academic certificates, ensuring efficiency and reducing manual intervention [3].

Smart contracts run on blockchain platforms like Ethereum, making them immutable and

tamper-proof. They eliminate the need for intermediaries, thereby reducing costs and enhancing trust. For example, when a university issues a certificate, a smart contract can automatically record it on the blockchain and generate a unique identifier for verification [4].

2.3 Digital Identity Management

Digital identity management refers to the process of securely managing user identities in digital systems. Blockchain technology has emerged as a powerful solution for digital identity due to its decentralized nature. In this project, students will use blockchain-based digital wallets to store and manage their academic credentials, giving them full ownership and control over their certificates [5].

Unlike traditional systems, blockchain-based identity management ensures that personal data is not stored on centralized servers, reducing the risk of breaches. It also allows for seamless and secure sharing of credentials with third parties, such as potential employers or academic institutions [6].

2.4 Blockchain for Credential Management

Using blockchain for credential management addresses many challenges associated with traditional systems, such as forgery, loss, and inefficient verification. When a certificate is issued on a blockchain, it is assigned a unique identifier, making it tamper-proof and easily verifiable. This project leverages these properties to create a secure, efficient, and transparent certificate management system [7].

Blockchain ensures that certificates are accessible to students and verifiable by third parties without intermediaries. By embedding certificates in a blockchain network, universities can guarantee their authenticity and eliminate the risk of unauthorized modifications [8].

2.5 Digital Wallets for Credential Management

A digital wallet is a software-based system that stores a userâs credentials, enabling secure access and sharing. In this project, students will use digital wallets to store their blockchain-based

certificates, granting them complete control over their credentials. These wallets use cryptographic keys to ensure secure access and sharing [9].

Digital wallets not only enhance security but also improve convenience. For instance, a student can share their certificate with a potential employer by providing a QR code or a link from their wallet. The employer can then verify the certificate on the blockchain without needing additional intermediaries [10].

2.6 QR Code-Based Verification

QR codes are a simple yet powerful tool for certificate verification. In this project, each certificate will include a QR code that links to its record on the blockchain. Verifiers can scan the QR code to instantly access the certificateâs details and confirm its authenticity [11].

QR codes eliminate the need for manual verification processes, making them ideal for a system where efficiency and user experience are critical. By combining QR codes with blockchain, this project ensures that certificates are both easily accessible and tamper-proof [12].

2.7 Security and Privacy in Blockchain Systems

Security and privacy in blockchain systems are ensured through decentralization, cryptographic mechanisms, and consensus protocols, making data tamper-proof and resilient to attacks. Features like public-private key cryptography secure authentication, while hash functions ensure data integrity. Despite these strengths, challenges persist, such as private key loss, 51 percent attacks, and vulnerabilities in smart contracts that can be exploited by malicious actors [13]. Additionally, social engineering and phishing attacks pose risks to users [14]. Mitigating these challenges requires robust security practices, including secure key management and regular auditing of smart contracts. Blockchainâs immutability and transparency offer robust privacy controls but must balance data accessibility with user confidentiality.

Chapter 3

Related Work

The application of blockchain technology in certificate management has garnered considerable attention globally. Several initiatives and research projects have explored blockchain's potential to create secure, immutable, and easily verifiable credential systems. This section reviews existing systems and highlights their relevance and limitations, particularly to the Bangladeshi context.

3.1 Sony Global Education's Blockchain Platform

Sony Global Education, in collaboration with IBM, has developed a blockchain-based platform designed for the secure storage and sharing of educational records [15]. This system aims to protect student achievements and facilitate the sharing of verified qualifications with third parties.

However, due to its proprietary nature, this platform may not be readily accessible or affordable for educational institutions in Bangladesh. The absence of open-source availability and potential licensing costs make it less suitable for implementation in resource-constrained environments common in developing countries.

3.2 EduCTX

EduCTX is a blockchain-based higher education credit platform proposed by TurkanoviÄ et al. [16]. It aspires to create a globally trusted system for managing and exchanging academic credits.

While EduCTX provides a framework for international credit transfer, its primary focus on the

European Credit Transfer and Accumulation System (ECTS) limits its direct applicability to the Bangladeshi education system, which operates under different accreditation standards and credit structures.

3.3 Digital Certificates in Bangladesh

Currently, some universities in Bangladesh have begun issuing digital certificates in PDF format. However, these certificates are often not secured and remain susceptible to forgery and unauthorized alterations [17]. The verification process continues to rely on direct contact with the issuing institution, resulting in delays and inefficiencies.

There is an evident need for a unified, secure, and efficient digital certificate management system in Bangladesh that leverages blockchain technology to address these challenges.

3.4 Justification for the Proposed Project

In light of these limitations, there is a clear necessity for a blockchain-based certificate management system tailored to the Bangladeshi context. The proposed project offers several key **advantages:**

- **Customization to Local Needs**: By concentrating on the specific requirements of Bangladeshi educational institutions, the system can be designed to align with local accreditation standards and administrative processes.
- **Resource Efficiency**: Developing an open-source solution considerate of resource constraints ensures that the system is accessible to institutions with limited technical and financial capabilities.
- **Enhanced Security and Trust**: Implementing a blockchain system addresses prevalent issues of certificate forgery and verification inefficiencies in Bangladesh, thereby enhancing the credibility of academic qualifications.
- **Ease of Adoption**: By offering a user-friendly interface and providing support for stakeholders, the system encourages adoption among universities, students, and employers, facilitating a smoother transition from traditional methods.

3.5 Contribution to the Bangladeshi Education Sector

The proposed project has the potential to significantly impact the Bangladeshi education sector by:

- **Modernizing Certificate Management**: Introducing advanced technology to streamline and secure certificate issuance and verification processes.
- **Supporting Digital Transformation**: Aligning with national initiatives toward digitization and contributing to the development of digital infrastructure in education.
- **Providing a Scalable Model**: Establishing a framework that can be expanded to other applications within the education system or replicated in similar contexts in other developing countries.

Chapter 4

Software Requirements Specification(SRS)

4.1 Functional Requirements

4.1.1 University Administration

Student Management: Add new students to the system by entering their details (e.g. name, student ID and program).

Certificate Generation: Input student details and program information to generate digital certificates.

Certificate Issuance: Issue certificates and link them to the respective student on the blockchain. Calculate a unique hash value for each certificate and store it on the blockchain.

4.1.2 Students

Login: Securely log in or sign up using authentication mechanisms tied to their digital wallet.

View Certificates: Access and view issued certificates stored in their digital wallet.

Share Certificates: Share a QR code or link containing the certificate's blockchain hash for verification.

4.1.3 Verifiers

Verification Portal: Access a public verification portal without any login/signup requirement.

Certificate Verification:

Verify the authenticity of a certificate by scanning a QR code or entering a unique certificate ID/hash on the portal.

Instant Validation:

Instantly retrieve certificate details and confirm their authenticity against blockchain records.

4.2 Non-Functional Requirements

Performance: The system should handle multiple certificate issuances concurrently. Verification should occur within a few seconds of scanning the QR code or entering the token.

Scalability: The blockchain should accommodate increasing numbers of certificates without performance degradation.

Security: Certificates must be tamper-proof and securely stored on the blockchain. Digital wallets should use private-public key cryptography for secure authentication.

Usability: The user interface for university admin, students, and verifiers should be intuitive.

4.3 Activity Diagram

University: The university serves as the primary issuer of certificates within the blockchain-based system. It uses a dedicated Ethereum blockchain node to securely generate certificates for students. Each certificate includes essential details like student information, course completion data, and a unique hash value. Once created, the certificates are digitally signed by the university and sent to the students' digital wallets. This ensures that certificates are immutable, tamper-proof, and easily accessible for future use.

Students: Students act as the custodians of their certificates, which are stored in their digital wallets. They can securely manage and share these certificates with third parties when required, such as during job applications or higher education admissions. Since the certificates are stored

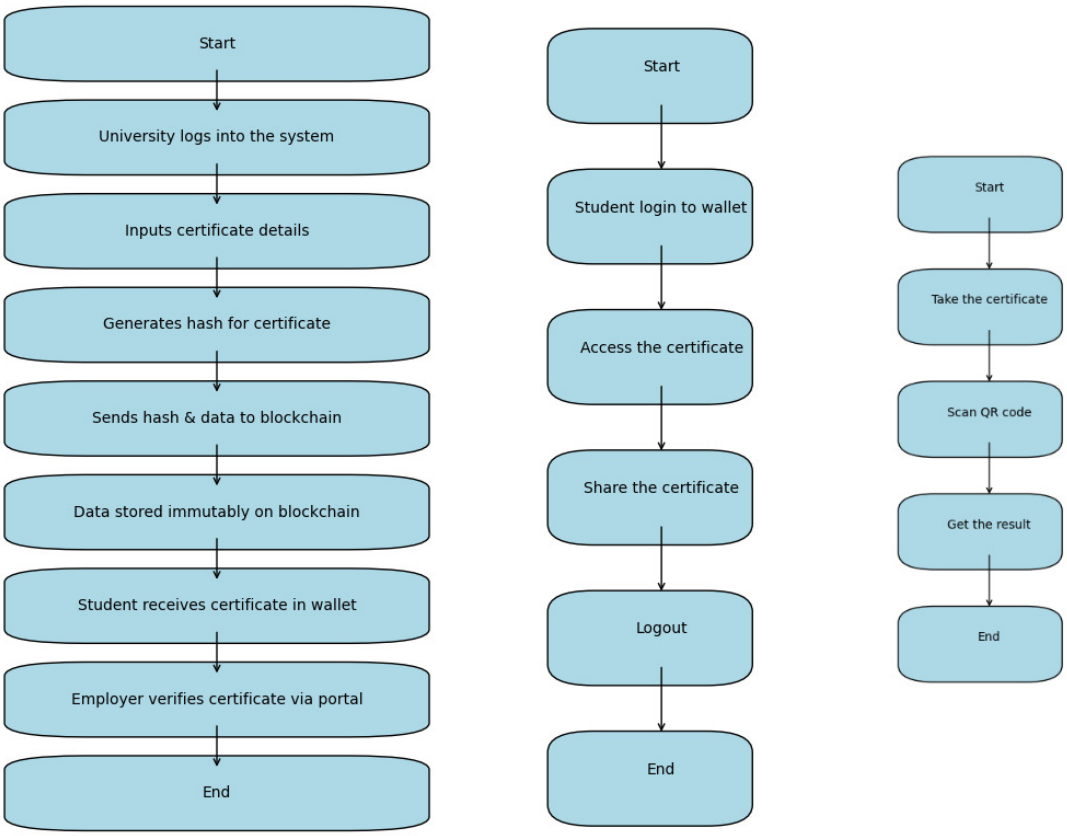

Figure 4.1: Activity Diagram(University, student and verifier respectively)

on the blockchain, students benefit from high security and authenticity. They also have access to a user-friendly interface to view and share their credentials without worrying about physical copies or forgery.

Verifier: The verifier, typically a company or institution, plays a crucial role in validating the authenticity of the certificates shared by students. They use the blockchain portal to verify the hash of the certificate against the records stored on the Ethereum blockchain. This process ensures that the certificate is genuine and unaltered, saving time and eliminating the need for manual verification. The decentralized nature of the blockchain guarantees trust and transparency in the verification process.

4.4 Use Case Diagram:

4.4.1 Use case scenario:

Certificate Issuance:

1. The administrator logs into the university's portal using their credentials.
2. Inputs certificate details.
3. The system generates a cryptographic hash (e.g., using SHA-256) of the certificate details to ensure integrity and immutability.
4. The system sends the hash and relevant certificate details to the Ethereum blockchain via a smart contract.
5. The smart contract records the data on the blockchain, ensuring it is secure and tamper-proof.
6. The certificate is linked to the student's digital wallet for future access.

Outcome: The certificate is securely stored on the Ethereum blockchain and made accessible to the student via their digital wallet.

Certificate Access by Students

1. The student accesses the system using their digital wallet, ensuring secure authentication.

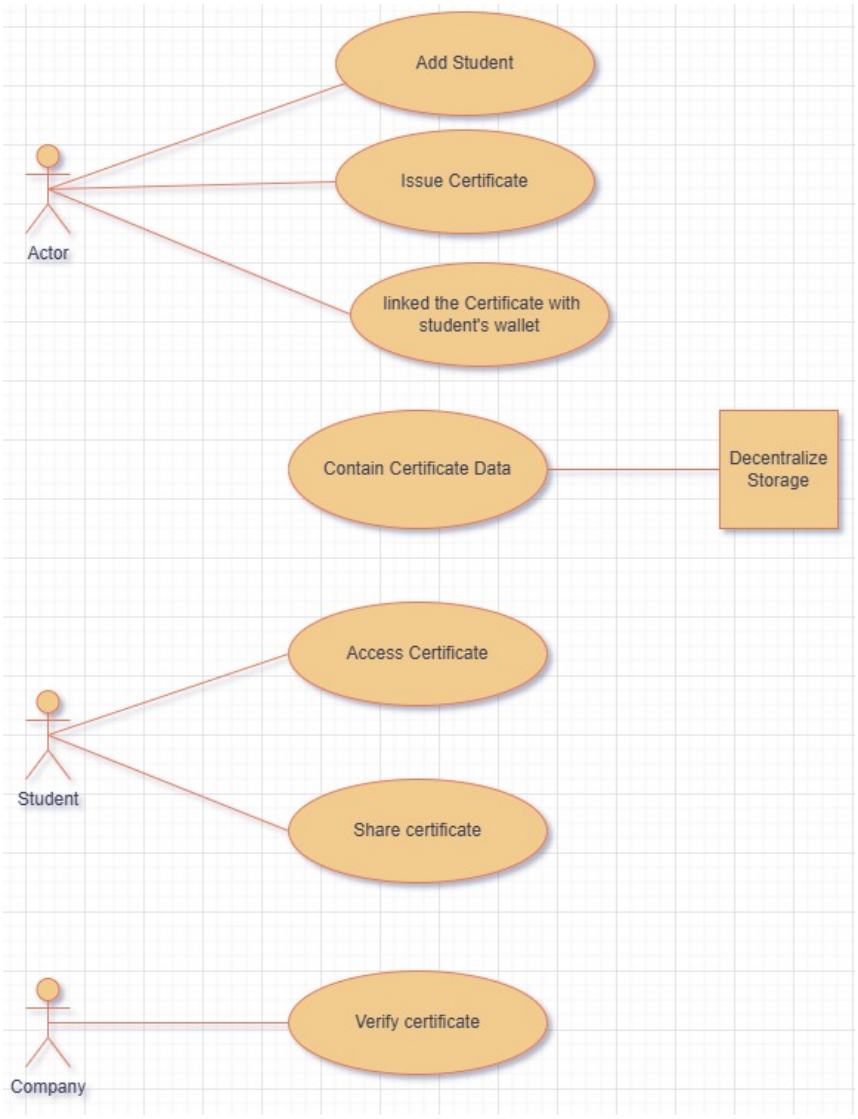

Figure 4.2: Use case Diagram

2. The system queries the blockchain to retrieve all certificates associated with the student's wallet address.

3. The retrieved certificate details, including the cryptographic hash and other metadata, are displayed on the student's dashboard.

4. The student can download the certificate or share it with stakeholders (e.g., employers, and educational institutions).

Outcome: The student securely accesses their certificates and shares them with stakeholders as needed.

Certificate Verification

1. The company or organization visits the certificate verification portal.

2. Inputs the certificate hash or unique certificate ID provided by the student.

3. The system uses a smart contract query to fetch the certificate details stored on the Ethereum blockchain.

4. The system compares the provided certificate details with the blockchain-stored data.

    - If matches and is created by the right node, the certificate is confirmed as authentic.
    - If not match, the certificate is flagged as invalid.

5. The verification result (authentic or invalid) is displayed to the third party in real-time.

Outcome: The third party verifies the authenticity of the certificate securely and efficiently.

Chapter 5

Design

5.1 System Architecture

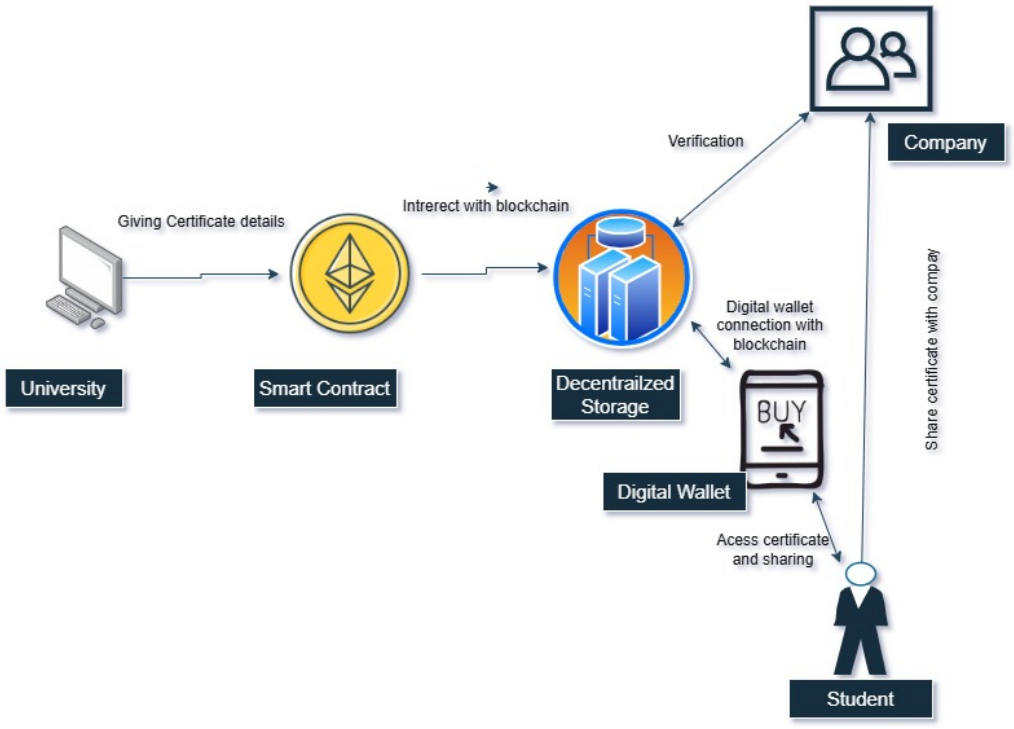

Figure 5.1: System Design

The architecture includes the following components:

1. **University Portal:** The administrator uses the portal to issue certificates, which are then

stored on the blockchain. It is integrated with the blockchain via smart contracts.

2. **Blockchain:** Ethereum blockchain is used to store certificates securely and immutably. The data is encrypted and stored with a unique identifier (hash) for each certificate.

3. **Digital Wallet"** The student's digital wallet holds the certificate and allows them to access and share it. It is linked to the blockchain.

4. **Verification Portal:** Third parties (e.g., employers) can verify certificates by accessing the portal, where they can input a certificate ID or hash to validate their authenticity or just by scanning QR code.

5.2 Data Flow Diagram

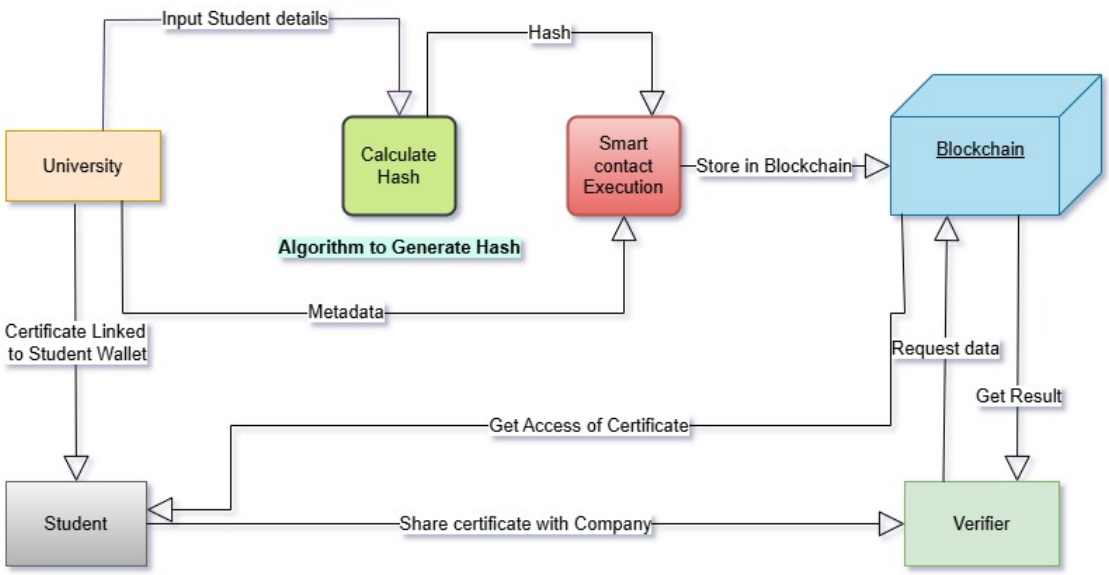

Figure 5.2: Data Flow Diagram

5.2.1 University Inputs Student Details

The process begins with the university administration, which is responsible for issuing certificates. The university collects all the necessary details related to the student. Details form the core

of the certificate, ensuring the information is accurate and comprehensive. The student details act as input data for the system and are critical to creating a unique and immutable certificate.

5.2.2 Calculate Hash (Using SHA-256 Algorithm)

Once the student details are gathered, they are passed into a hashing algorithm, specifically SHA-256. This step ensures that a unique, fixed-length hash value is generated from the input data. The hash acts as a digital fingerprint for the certificate, guaranteeing that any minor alteration in the input data would result in a completely different hash value. The SHA-256 algorithm is widely used for its cryptographic strength and ensures data integrity.

This hash is an essential component of the system because it serves as the immutable representation of the certificate and is later stored on the blockchain.

5.2.3 Smart Contract Execution

After the hash is generated, the next step involves interacting with a smart contract deployed on the Ethereum blockchain. The smart contract is a self-executing program that automates the process of storing the certificate data securely on the blockchain. The university provides the hash and additional metadata (such as the course name, issue date, and institution name) as input to the smart contract.

The smart contract ensures that:

- The data is recorded immutably on the blockchain.
- The metadata and hash are stored in a decentralized manner, making them tamper-proof.
- Only authorized entities, such as the university, can add data to the blockchain.

The smart contract acts as the bridge between the university and the blockchain, ensuring data security and transparency.

5.2.4 Store Data in Blockchain

Once the smart contract is executed, the certificate hash and metadata are permanently stored in the blockchain. The blockchainâs decentralized nature ensures that the data is distributed across

multiple nodes, making it immune to tampering or unauthorized modifications. This storage step is critical because it guarantees the authenticity and security of the certificate data.

The blockchain stores:

- **Hash**: The unique digital fingerprint of the certificate.
- **Metadata**: Details about the certificate, such as the issuing institution, issue date etc.

The blockchainâs immutable storage mechanism ensures that the certificate data is always available for verification and cannot be altered once recorded.

5.2.5 Certificate Linked to Student Wallet

Once the certificate data is stored on the blockchain, univerisity with the help of the system links it to the studentâs digital wallet. The wallet serves as a repository for the studentâs certificates, allowing them to access and manage their credentials easily. A reference to the certificate such as a transaction ID or the metadata stored on the blockchain is sent to the studentâs wallet.

This step ensures that students can:

- View their certificates anytime.
- Share their certificates with third parties such as employers or academic institutions.

By integrating certificates into the studentâs digital wallet, the system enhances accessibility and convenience.

5.2.6 Verifier Requests Certificate Access

When a verifier (such as a company or academic institution) needs to authenticate a studentâs certificate, they initiate a request. The verifier uses the certificate reference provided by the student, such as the hash value or QR code to query the blockchain.

The verifier interacts with the blockchain by:

- Accessing the certificate hash and metadata stored on the blockchain.
- Sending the certificate details to the smart contract for validation.

5.2.7 Blockchain Verification

The smart contract retrieves the certificate data stored on the blockchain and compares it with the input data provided by the verifier. If the input hash matches the hash stored on the blockchain, the certificate is deemed valid. If the hashes do not match, the system flags the certificate as invalid.

This verification process ensures:

- The authenticity of the certificate.
- Protection against forgery or tampering.

The blockchainâs decentralized architecture ensures that the verification process is transparent and reliable.

5.2.8 Sharing Certificate with Companies

The student can also share their certificate details with companies or third parties. By providing access to their digital wallet or sharing the certificate hash, students can prove the authenticity of their credentials efficiently. This process eliminates the need for lengthy manual verification processes and fosters trust between students and employers.

Chapter 6

Development Planning

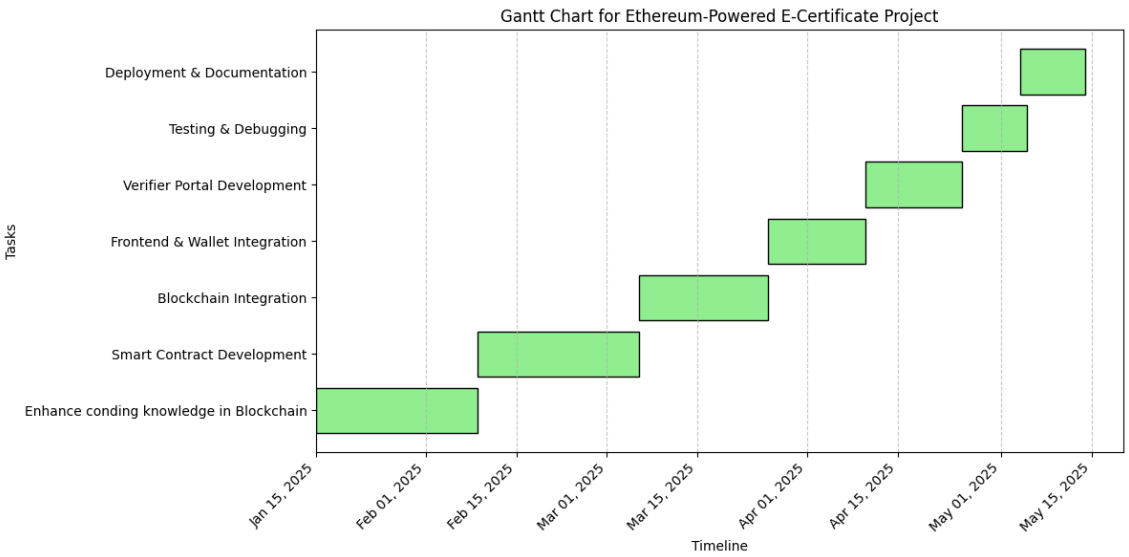

Figure 6.1: Gantt Chart

6.1 Gantt Chart

6.1.1 Phase 1: Enhance conding knowledge in Blockchain

Duration: January 15 - February 9, 2025

Activities:

- Gain hands-on experience with Solidity.

- Develop and test basic smart contract functionality.
- Familiarize with Ethereum blockchain tools like Remix, Ganache and MetaMask.

6.1.2 Phase 2: Smart Contract Development

Duration: February 9 - March 6, 2025

Activities:

- Develop the core smart contracts for certificate creation, storage and retrieval.
- Write code for hashing certificate data using SHA-256.
- Implement metadata storage and certificate linking to student wallets.
- Test contract logic extensively.

6.1.3 Phase 3: Blockchain Integration

Duration: March 6 - March 26, 2025

Activities:

- Deploy smart contracts to the Ethereum blockchain.
- Set up a blockchain environment for development and testing (e.g., using a local test network or Goerli testnet).
- Integrate blockchain with backend services for certificate issuance.

6.1.4 Phase 4: Frontend & Wallet Integration

Duration: March 26 - April 10, 2025

Activities:

- Design and develop a web interface for the university to create and issue certificates.
- Implement wallet integration for students to receive certificates.
- Ensure smooth interaction between the frontend, wallet and blockchain backend.

6.1.5 Phase 5: Verifier Portal Development

Duration: April 10 - April 25, 2025

Activities:

- Create a portal for verifiers (e.g., companies) to validate certificates.
- Implement logic to fetch and verify hashes stored on the blockchain.
- Ensure user-friendly functionality for data validation.

6.1.6 Phase 6: Testing & Debugging

Duration: April 25 - May 4, 2025

Activities:

- Test each component (frontend, backend and blockchain) individually and as an integrated system.
- Debug issues related to smart contract execution, data flow and UI/UX.
- Test wallet functionality and verifier portal thoroughly.

6.1.7 Phase 7: Deployment & Documentation

Duration: May 11 - May 31, 2025

Activities:

- Deploy the system to a live environment.
- Write comprehensive documentation, including user manuals and technical details.
- Prepare and rehearse a final project presentation.

6.2 Hardware Requirements

6.2.1 For Development

Developer Machines:

- **Processor:** Intel Core i5 or AMD Ryzen 5 (or higher).
- **RAM:** 8 GB or more for smooth multitasking and blockchain testing.
- **Storage:** 512 GB SSD or higher for fast data access and storage.
- **Graphics Card:** Integrated or dedicated GPU for rendering and UI testing.

6.2.2 User Requirements

Devices for users (students, verifier):

- Smartphones, Tablets, or Laptops with modern web browsers.
- MetaMask-Compatible Devices for wallet interaction.

6.3 Software Requirements

Blockchain Development Tools:

- Truffle or Hardhat for smart contract development and testing.
- Ganache for simulating a local blockchain network.

Package Managers:

- Node.js and npm/yarn for managing JavaScript dependencies.

6.3.1 Programming Languages and Libraries

Smart Contracts:

- Solidity for creating and deploying blockchain contracts.

Frontend:

- React.js for building the web application.
- Web3.js or ethers.js for blockchain interaction.

Backend:

- Node.js for server-side programming.
- JSON Web Tokens (JWT) for authentication.

Blockchain and Wallets:

- Ethereum for public blockchain infrastructure.
- MetaMask for wallet integration.

QR Code Libraries:

- QRCode.js or similar for generating and rendering QR codes.
- Reportlab to generate instant PDF.

6.3.2 Hosting and Deployment

Frontend Hosting:

- Vercel, Netlify, or AWS for deploying the web application.

Smart Contract Deployment:

- Ethereum testnets (e.g., Rinkeby, Goerli) for testing.
- Ethereum mainnet for production.

Chapter 7

Conclusion

In conclusion, the proposed blockchain-based certificate management system represents a transformative approach to the generation, issuance, management, and verification of academic certificates within universities. By utilizing the Ethereum public blockchain platform, this project prioritizes transparency, security, and authenticity, while empowering students to maintain control over their academic credentials through digital wallets. The inclusion of a third-party verification portal is designed to further bolster trust in the system, offering significant advantages to both employers and educational institutions. With a development timeline of four months, this project is committed to delivering a com prehensive and user-friendly solution to the current challenges in certificate management. Empha sizing scalability, security, and efficiency, the system leverages cutting-edge technologies such as Solidity and Ethereum. The anticipated success of this initiative is expected to demonstrate the practical application of blockchain technology in education, significantly enhancing the processes of certificate issuance, management, and verification in the digital era. Ultimately, this project not only highlights the potential of blockchain in real-world scenarios but also sets the stage for future advancements in the field of academic credentialing.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, white paper.

[2] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[3] V. Buterin, "A next-generation smart contract and decentralized application platform," 2013, ethereum white paper.

[4] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[5] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," *2015 IEEE Security and Privacy Workshops*, pp. 180–184, 2015.

[6] P. Dunphy and F. A. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 20–29, 2018.

[7] A. Grech and A. F. Camilleri, "Blockchain in education," 2017, european Commission report.

[8] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation, and reward," *Proceedings of the 11th European Conference on Technology Enhanced Learning*, pp. 490–496, 2016.

[9] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learning Environments*, vol. 5, no. 1, pp. 1–10, 2018.

[10] A. Vazirani and B. Chandavarkar, "Credential storage and sharing using blockchain wallets," *Journal of Innovation and Applied Technology*, vol. 6, no. 2, pp. 59–68, 2020.

[11] D. Hussein and A. Koubaa, "Qr-based verification for blockchain certificates," *Journal of Computer Science*, vol. 17, no. 4, pp. 427–439, 2021.

[12] M. Wazid, A. K. Das, and A. V. Vasilakos, "Authenticated key management protocol for iot-enabled devices using qr codes," *Journal of Information Security and Applications*, vol. 32, pp. 27–42, 2017.

[13] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," *2015 IEEE Symposium on Security and Privacy*, pp. 104–121, 2015.

[14] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of blockchain technology," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 106–134, 2018.

[15] S. Corporation, "Sony global education develops technology using blockchain for open sharing of academic proficiency and progress records," https://www.sony.net/SonyInfo/News/Press/201608/16-071E/, 2016, accessed: October 1, 2023.

[16] M. TurkanoviÄ, M. HÃ¶lbl, K. KoÅ¡iÄ, M. HeriÄko, and A. KamiÅ¡aliÄ, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.

[17] M. N. M. Islam and M. M. Rahman, "Digital certificate verification system in bangladesh: Challenges and opportunities," *International Journal of Digital Society*, vol. 11, no. 1, pp. 1504–1510, 2020.