ACADEMIC CREDENTIAL VERIFICATION SYSTEM

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Use Case Report

submitted by

R. Tulasi Lakshmi

23505A0511

Under the guidance of

Mr. A. Prashant, Asst. Prof.

Department of Computer Science and Engineering

Prasad V. Potluri Siddhartha Institute of Technology

(Permanently affiliated to JNTU-Kakinada, Approved by AICTE)

(An NBA & NAAC accredited and ISO 9001:2015 certified institute)

Kanuru, Vijayawada-520 007

2024-2025

Prasad V. Potluri Siddhartha Institute of Technology

(Permanently affiliated to JNTU-Kakinada, Approved by AICTE)

(An NBA & NAAC accredited and ISO 9001:2015 certified institute)

Kanuru, Vijayawada-520 007

CERTIFICATE

This is to certify that the Use Case report entitled **"Academic Credential Verification"** that is being submitted by **R.Tulasi Lakshmi(23505A0511)**, as part of Assignment-1 and Assignment-2 for the **Blockchain Technology**(**20CS4601C)** course in **3-2** during the academic year **2024-2025**.

Course Coordinator	**Head of the Department**
Mr. A. Prashant	**Dr. A. Jayalakshmi**
Assistant Professor,	Professor and Head,
Department of CSE,	Department of CSE,
PVPSIT, Vijayawada	PVPSIT, Vijayawada

MARKS
ASSIGNMENT-1:_____ /5
ASSIGNMENT-2:_____ /5

INDEX

S. No.	Chapter	Page No.
1	Introduction	1
2	Background	2
3	Blockchain Basics	5
4	Use Case Overview	7
5	Implementation	10
6	Benefits	14
7	Challenges	16
8	Conclusion	17
9	SDG’s Addressed	18
10	References	19
11	Appendix A	20

1. INTRODUCTION

1.1. Overview of Blockchain Technology

Blockchain technology is a decentralized and distributed ledger system that records transactions across multiple nodes, ensuring transparency, security, and immutability. Unlike traditional databases, blockchain operates on a peer-to-peer network, eliminating the need for central authorities. Each block in the chain contains a cryptographic hash of the previous block, making data tampering virtually impossible. Originally designed for cryptocurrency transactions, blockchain has now expanded into various domains, including finance, supply chain, healthcare, and digital warranty management.

1.2. Relevance of Blockchain in Academic Credential Verification

Traditional methods of academic credential verification depend on centralized databases and physical documents, which often lead to inefficiencies such as credential fraud, prolonged authentication processes, and misplacement of records. Blockchain technology offers a solution by introducing a decentralized, secure, and transparent method for managing academic credentials.

A blockchain-powered credentialing system ensures the authenticity of academic qualifications by providing a permanent and tamper-resistant record. Smart contracts facilitate the automatic issuance and validation of credentials, reducing reliance on intermediaries and minimizing verification delays. Moreover, decentralized identifiers (DIDs) grant students direct access to their credentials, enabling effortless sharing with institutions and potential employers.

Integrating blockchain into academic credential authentication fosters a more reliable and fraud-proof system, strengthening the credibility of issued qualifications. By ensuring that records remain permanently verifiable, blockchain enhances trust in the academic and professional landscape while also streamlining administrative processes.

Additionally, blockchain's decentralized architecture eliminates risks associated with centralized data storage, such as unauthorized alterations or data loss. This is particularly beneficial for universities, certification authorities, and hiring organizations, as it simplifies credential validation without dependence on third-party verification services. Furthermore, blockchain-based credential records can be seamlessly transferred across institutions, ensuring continuity in a student's educational journey. As digital transformation advances in the education sector, blockchain-based verification systems emerge as an innovative and sustainable approach to securing and managing academic records with greater efficiency and reliability.

2. BACKGROUND

Traditional methods of verifying academic credentials come with several limitations that can result in inefficiencies, fraud risks, and administrative burdens. These issues stem from reliance on paper-based certificates, centralized databases, and manual verification processes. Below are some key challenges associated with the current academic credential verification systems:

2.1. Risk of Document Loss or Damage

Many institutions still issue paper-based degree certificates and transcripts, which are susceptible to loss, damage, or misplacement. Retrieving duplicate copies often involves lengthy administrative procedures, causing inconvenience for students and delays in verification processes.

2.2. Credential Fraud and Forgery

The prevalence of forged academic certificates poses a major challenge in the verification process. Employers and universities frequently encounter fraudulent claims due to the lack of a secure and standardized method of verifying the authenticity of academic credentials, leading to a loss of trust in issued qualifications.

2.3. Inefficient and Time-Consuming Verification

Academic credential verification often requires institutions to manually process verification requests, which can be slow and resource-intensive. Employers and higher education institutions must rely on third-party verification agencies or direct communication with issuing institutions, leading to delays and administrative overhead.

2.4. Limited Transparency and Traceability

With credentials stored in centralized systems, tracking changes in student records, ownership transfers, or modifications is difficult. This lack of transparency results in disputes and inconsistencies when verifying academic history, particularly in cases of international credential evaluation.

2.5. Challenges in Cross-Institutional Recognition

When students transfer between universities or apply for jobs in different countries, credential recognition can become a complex process. Institutions may have varying standards and verification methods, making it difficult to ensure seamless recognition of qualifications across different educational and professional domains.

By implementing blockchain technology in academic credential verification, these issues can be mitigated, ensuring secure, tamper-proof, and easily verifiable academic records while reducing administrative burdens and enhancing trust in the education system.

2.6. Security Risks and Data Tampering

Academic records stored in centralized databases are vulnerable to cyber threats, unauthorized modifications, and data breaches. Malicious actors can manipulate records, falsify qualifications, or delete crucial data, resulting in credibility issues for institutions and challenges for employers in verifying academic history.

2.7. Difficulty in Managing Global Credential Verification

With the rise in global education and employment opportunities, verifying credentials across borders has become increasingly complex. Different institutions follow varying standards for credential issuance and validation, making it difficult for employers and universities to authenticate records efficiently and consistently.

2.8. Discrepancies Between Institutions and Employers

Conflicts often arise between educational institutions and hiring organizations regarding credential authenticity. Due to the lack of a universal verification system, employers must rely on time-consuming background checks or third-party verification services, leading to delays in recruitment and admissions processes.

2.9. Limited Student Access to Credential Information

Many traditional verification systems do not provide students with direct access to their academic records. Graduates often need to request transcripts from their universities, causing delays in job applications and further studies. Additionally, the lack of real-time tracking makes it difficult to confirm the validity of credentials instantly.

2.10. Absence of Automated Expiry and Renewal Notifications

Some certifications and licenses require periodic renewals, but traditional systems do not provide automated reminders. This results in students and professionals missing renewal deadlines, leading to unnecessary complications in career advancements or compliance requirements.

Given these challenges, a secure, transparent, and automated credential verification system is essential. Blockchain technology offers a decentralized, tamper-proof solution that enhances trust, improves efficiency, and provides a seamless verification experience for students, institutions, and employers alike.

3. BLOCKCHAIN BASICS

Blockchain technology is a distributed ledger system that ensures secure, transparent, and tamper-proof transactions. Unlike traditional systems that rely on intermediaries, blockchain enables trustless peer-to-peer interactions, reducing the need for third parties in financial transactions, supply chain management, and digital warranty verification. Its decentralized nature enhances security and transparency, making it an ideal solution for many industries. Below are the key concepts that define blockchain technology:

3.1. Decentralization

Traditional databases are managed by centralized authorities, such as banks or corporations, which creates a single point of failure and makes them vulnerable to hacks or data manipulation. Blockchain, on the other hand, operates on a decentralized network, where multiple independent nodes validate and store data. This ensures that no single entity has full control over the system, making it resistant to censorship and fraud. Additionally, decentralized structures provide greater security, as compromising one node does not affect the integrity of the entire network. Since all transactions are recorded and verified across multiple nodes, blockchain also enhances transparency, allowing participants to independently verify transactions.

3.2. Immutability

One of blockchain's defining characteristics is immutability, meaning once a transaction is recorded, it cannot be altered or deleted. This is achieved through cryptographic hashing, where each block is linked to the previous one, forming a secure chain that prevents unauthorized modifications. The integrity of the blockchain is maintained through consensus mechanisms, ensuring that all network participants agree before new data is added. Since tampering with a single block would require modifying all subsequent blocks—an operation that demands enormous computational power—fraud and unauthorized changes become nearly impossible. This feature makes blockchain particularly useful for audit trails, financial transactions, and warranty tracking.

3.3. Transparency

Blockchain transactions are publicly verifiable, meaning anyone with access to the network can audit the transaction history. This transparency is ensured by distributed ledger technology (DLT), where every participant has access to an identical copy of the data, eliminating the risk of hidden alterations. Public blockchains, such as Bitcoin and Ethereum, offer complete transparency, fostering trust among users. This openness reduces the possibility of corruption and fraudulent activities, as any attempt to manipulate records would be instantly detected by the network.

3.4. Smart Contracts

Smart contracts are self-executing contracts with predefined conditions embedded in the blockchain. Once the specified conditions are met, the contract automatically executes the agreed-upon actions, eliminating the need for manual processing. This automation ensures trustless execution, reducing fraud and disputes between parties. By removing intermediaries, smart contracts also lower operational costs and increase efficiency. In the context of a digital warranty system, smart contracts can automatically transfer warranty ownership, validate claims, and process warranty expirations without human intervention.

3.5. Consensus Mechanisms

Blockchain networks rely on consensus mechanisms to validate transactions and maintain system integrity. The most widely used mechanism is Proof of Work (PoW), where miners solve complex mathematical puzzles to confirm transactions, as seen in Bitcoin. Another approach, Proof of Stake (PoS), selects validators based on the number of tokens they hold, which is used in Ethereum 2.0. A more efficient variation, Delegated Proof of Stake (DPoS), involves electing a smaller group of nodes to verify transactions, improving scalability and reducing energy consumption. These consensus models prevent malicious actors from manipulating the system and ensure that only valid transactions are recorded on the blockchain.

3.6. Cryptographic Security

Blockchain security relies on advanced cryptographic techniques to protect user data and transactions. Each transaction is authenticated using public and private keys, ensuring that only authorized individuals can initiate transactions. Hash functions further enhance security by converting data into fixed-length unique codes, making it nearly impossible to reverse-engineer original information. Additionally, blockchain uses encryption to protect sensitive data, ensuring that unauthorized users cannot access confidential records. This high level of security makes blockchain an ideal technology for digital warranties, financial transactions, and identity management.

By combining these key features—decentralization, immutability, transparency, smart contracts, and cryptographic security—blockchain provides a robust and efficient foundation for various industries, including digital warranty management.

4. USE CASE OVERVIEW

The use case for a Blockchain-Based Academic Credential Verification System aims to modernize the verification process by leveraging blockchain technology. This system ensures secure, transparent, and fraud-resistant issuance, validation, and transferability of academic credentials.

4.1. Objectives

The primary goal of this blockchain-based system is to replace traditional paper-based certificates with a digital credential management platform. Conventional degree verification processes involve manual authentication, which is slow, inefficient, and prone to document forgery. By utilizing blockchain, academic records can be securely stored, instantly verifiable, and easily accessible anytime.

A major challenge in credential verification is the prevalence of fake degrees and falsified academic transcripts. Blockchain's immutability ensures that once a credential is issued, it cannot be altered or forged, significantly reducing fraud. This strengthens trust between educational institutions, employers, and students while maintaining the integrity of issued credentials.

Another critical aspect is enabling seamless credential portability. Blockchain allows students to store and share their verified records securely, reducing dependency on third-party verification services. This automation simplifies applications for higher education, employment, and professional licensing.

The system also enhances verification efficiency by automating validation. Smart contracts instantly confirm the authenticity of academic credentials, reducing processing time and eliminating the need for intermediaries. This leads to quicker decision-making in hiring, admissions, and certification approvals.

Transparency is another key benefit of blockchain-based credential verification. Universities, employers, and credential holders can access real-time academic records through a decentralized network, reducing disputes over credential authenticity. The system provides all stakeholders with secure, tamper-proof access to academic qualifications.

4.2. Scope of the System

The blockchain-based warranty system focuses on securing, managing, and transferring digital warranties. The system includes:

The blockchain-based credential verification system focuses on securing, managing, and authenticating digital academic records. The system includes:

1. **Educational Institutions (Universities, Colleges, Schools):** Issue digital credentials stored on the blockchain.
2. **Students and Graduates:** Securely manage their credentials and share them with employers or institutions.
3. **Employers and Verification Agencies:** Instantly validate academic qualifications without relying on centralized databases.
4. **Blockchain Network:** Ensures transparent, tamper-proof record storage and smart contract execution.

4.3. System Architecture

The architecture of the Blockchain-Based Credential Verification System consists of the following components:

4.3.1. User Layer

This layer includes the primary participants who interact with the system:

- **Educational Institutions:**
    - Register as authorized issuers of credentials.
    - Issue blockchain-verified degrees, diplomas, and certificates.
- **Students and Graduates:**
    - Securely access and share their verified academic credentials.
    - Control permissions for third-party verification requests.
- **Employers and Verification Bodies:**
    - Instantly authenticate credentials without requiring direct institution involvement.
    - Reduce the time and effort spent on background checks.

4.3.2. Web Application Layer

This layer facilitates interaction between users and the blockchain network:

- **User Dashboard:**
    - Allows institutions to issue, manage, and track digital credentials.
    - Provides students with access to their credential records.
    - Enables employers to verify academic qualifications in real time.
- **Credential Management System:**
    - Handles user authentication and role-based access.
    - Connects users securely to blockchain-based credential storage.

4.3.3. Blockchain Layer

This layer ensures the security and integrity of credential transactions:

- **Smart Contract Mechanism:**
    - **Credential Record Contract:**
        - Stores credential details such as issuing institution, recipient, degree information, and date of issuance.
        - Governs the issuance, verification, and ownership of digital credentials.
    - **Automated Execution:**
        - When a university issues a credential, it is recorded permanently on the blockchain.
        - When a student shares credentials, an employer can verify authenticity instantly.
- **Decentralized Ledger:**
    - Maintains a secure, tamper-proof record of all issued academic credentials.
    - Prevents unauthorized alterations, ensuring the integrity of stored data.

By implementing these blockchain-based components, the system ensures a more secure, transparent, and efficient process for academic credential verification, benefiting students, institutions, and employers alike.

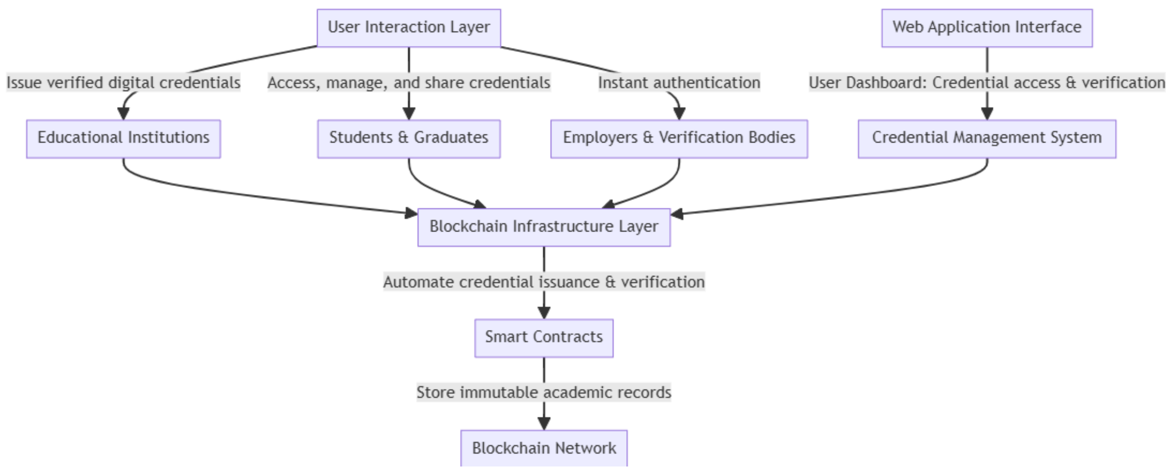

Figure 4.1: Architecture of Blockchain based Academic Credential Verification

5.IMPLEMENTATION

5.1. Setting Up the Blockchain Environment

To implement the EduBlock academic credential verification system,
blockchain environment must be configured using Ethereum. Essential tools include:

- Truffle – A development framework for Ethereum smart contracts.
- Ganache – A local Ethereum blockchain for testing.
- MetaMask – A browser extension for managing Ethereum accounts and transactions.
- Solidity (v0.8.19) – The programming language used to write smart contracts, ensuring security features like overflow protection and enhanced error handling.

Once the environment is set up, developers can proceed with writing smart contracts for issuing, storing, and verifying academic credentials.

5.2. Defining Smart Contracts

5.2.1. Writing the Smart Contract for Warranty Management

The **Credential** contract is responsible for issuing, transferring, and verifying academic credentials. It defines a Credential struct, which holds essential details such as:

- Credential ID
- Issuing institution
- Recipient (student)
- Issue date
- Expiration date (if applicable)
- Degree/Certification details

The contract also maintains mappings for registered institutions, issued credentials, and ownership tracking.

```
struct Credential {
    uint256 id;
    address issuer;
    address owner;
    uint256 issuedAt;
    uint256 validUntil;
    string degreeDetails;
}

mapping(address => bool) internal registeredInstitutions;
mapping(uint256 => Credential) internal credentials;
mapping(address => uint256[]) internal ownerToCredentials;
```

5.2.2. Registering Institutions

To prevent unauthorized entities from issuing credentials, institutions must register their blockchain addresses before they can issue digital certificates.

```
function registerInstitution() external {
    require(!registeredInstitutions[msg.sender], "Already registered");
    registeredInstitutions[msg.sender] = true;
}
```

5.2.3. Issuing Academic Credentials

Once registered, institutions can issue digital credentials to students. When issuing a credential, the institution specifies the student's blockchain address, degree details, and validity (if applicable).

```
function issueCredential(address to, uint256 validUntil, string memory degreeDetails) externa
    require(to != address(0), "Invalid recipient");

    uint256 credentialId = nextCredentialId++;
    credentials[credentialId] = Credential({
        id: credentialId,
        issuer: msg.sender,
        owner: to,
        issuedAt: block.timestamp,
        validUntil: validUntil,
        degreeDetails: degreeDetails
    });

    ownerToCredentials[to].push(credentialId)
}
```

5.2.4. Viewing a Student's Credentials

Students should be able to view their academic records at any time. This provides transparency and allows students to manage their academic records.

```
function viewCredentials() external view returns (Credential[] memory) {
    uint256[] memory credentialIds = ownerToCredentials[msg.sender];
    Credential[] memory ownedCredentials = new Credential[](credentialIds.length);

    for (uint256 i = 0; i < credentialIds.length; i++) {
        ownedCredentials[i] = credentials[credentialIds[i]];
    }

    return ownedCredentials;
}
```

5.2.5. Verifying Credential Validity

Employers or other institutions may need to verify if a credential is still valid. This prevents the misuse of expired academic credentials.

```
function verifyCredential(uint256 credentialId) external view returns (bool) {
    return block.timestamp <= credentials[credentialId].validUntil;
}
```

5.2.6. Transferring Credentials (For Academic Partnerships or Migrations)

If a student transfers to another institution, they may need to transfer their credentials. The system allows for the controlled transfer of credentials. This ensures academic records remain accurate and transferable without fraud.

```
function transferCredential(uint256 credentialId, address newOwner) external {
    require(credentials[credentialId].owner == msg.sender, "Not the owner");
    require(newOwner != address(0), "Invalid new owner");

    credentials[credentialId].owner = newOwner;
    ownerToCredentials[newOwner].push(credentialId);
}
```

5.3. Deploying and Integrating with a Frontend

After testing the smart contract using **Ganache**, the next step is deploying it to an Ethereum test network (such as **Goerli** or **Sepolia**) before moving to the **Ethereum Mainnet**.
The frontend is built using **React.js** with **Web3.js** or **Ethers.js** for blockchain interactions. The interface allows users to:

- Institutions to register and issue credentials.
- Students to view and manage their credentials.
- Employers to verify academic qualifications.

This user-friendly interface ensures secure and efficient academic credential management, eliminating the need for manual verification processes.

5.4. Workflow:

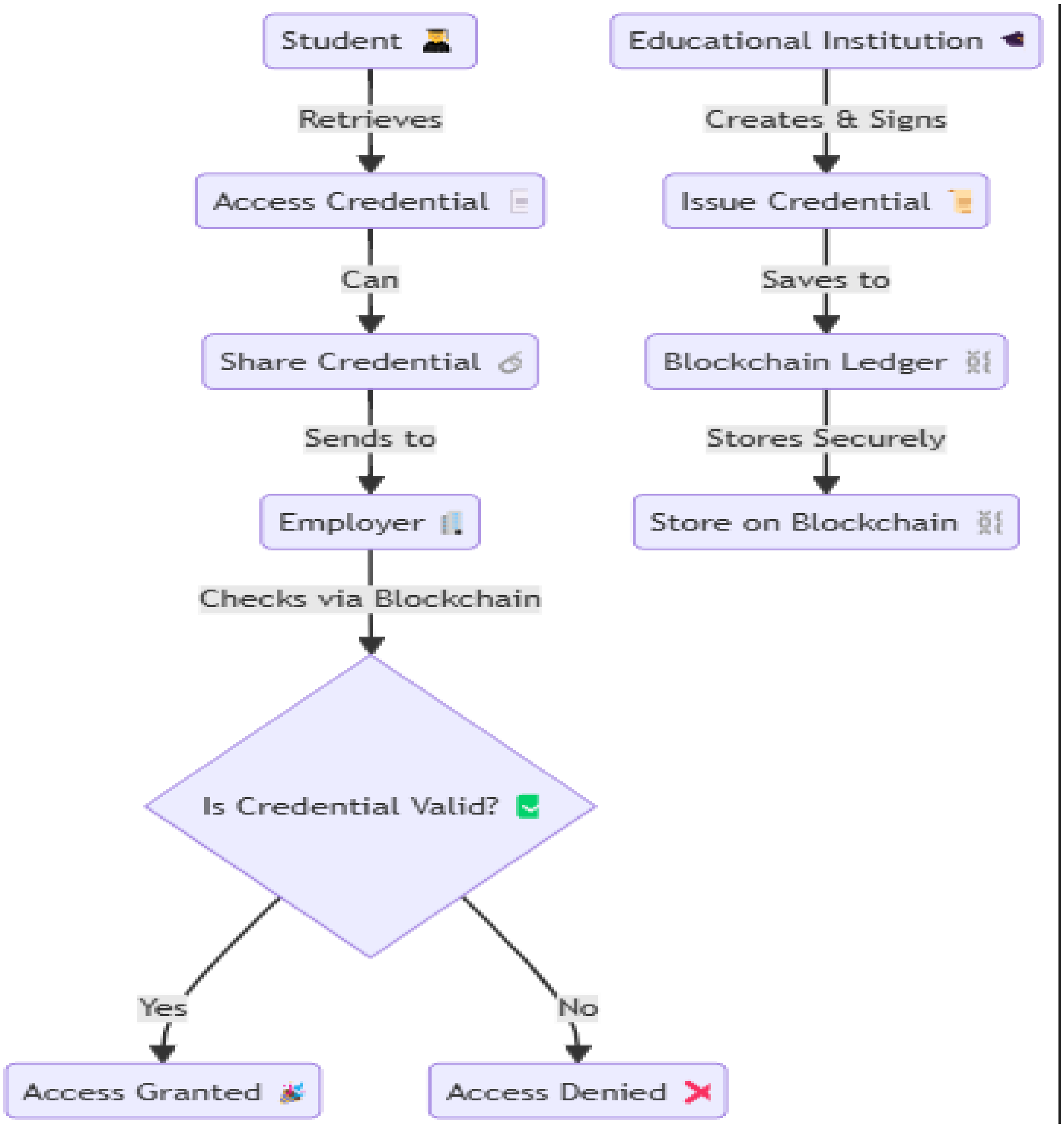

Figure 5.1: Workflow of Blockchain based Academic Credential Verification System

6. BENEFITS OF BLOCKCHAIN FOR ACADEMIC CREDENTIAL VERIFICATION

Blockchain technology enhances academic credential verification by introducing transparency, security, and automation. Traditional credential verification systems rely on centralized databases, making them vulnerable to fraud, inefficiency, and data loss. By leveraging blockchain, credential verification becomes tamper-proof, cost-effective, and highly efficient. Below are the key advantages:

6.1. Enhanced Security and Immutability

Blockchain provides immutable records, ensuring that once an academic credential is issued, it cannot be altered or deleted. This prevents credential forgery and ensures that all records remain tamper-proof. The cryptographic nature of blockchain secures sensitive educational data, reducing risks of hacking and unauthorized modifications.

6.2. Elimination of Fake Degrees and Credentials

A major issue in traditional credential verification is the creation of fake degrees and falsified academic records. With blockchain, each credential is stored as a unique, verifiable token that can be easily validated. This prevents diploma mills and unauthorized claims, enhancing trust among employers, institutions, and students.

6.3. Transparency and Auditability

Blockchain-based credential verification provides real-time access to academic records for employers, institutions, and other stakeholders. Since all transactions are recorded on a distributed ledger, any party can verify a credential's authenticity without relying on intermediaries. This transparency reduces disputes and increases trust in the verification system.

6.4. Easy Transferability of Academic Records

Traditionally, transferring academic records between institutions or verifying them for employment requires extensive paperwork. With blockchain, academic credentials are easily transferable between authorized entities. Students can share their verified records instantly without needing approval from multiple institutions.

6.5. Cost Reduction and Efficiency

Blockchain significantly reduces administrative costs associated with academic credential verification. Since all records are stored on-chain, there is no need for manual verification, paperwork, or intermediaries, leading to faster validation and lower operational expenses for institutions and employers.

6.6. Smart Contracts for Automated Credential Validation

Smart contracts automate credential validation by ensuring that academic qualifications meet predefined criteria. When a verification request is made, the smart contract checks the record's authenticity and issues instant validation, reducing processing time and human errors.

6.7. Preventing Credential Fraud and Unauthorized Claims

A key benefit of blockchain is preventing academic fraud by ensuring that credentials cannot be manipulated. Fake degree claims, altered transcripts, and other forms of academic dishonesty are eliminated since the blockchain ledger maintains a permanent, unchangeable history of all issued credentials.

6.8. Scalability and Integration with Digital Learning Platforms

Blockchain-based credential systems can integrate with online learning platforms, MOOCs (Massive Open Online Courses), and universities to issue digital certificates automatically. This ensures that students and professionals can securely store and share their verified credentials without manual intervention.

6.9. Increased Trust Among Employers and Institutions

A transparent and fraud-resistant credential verification system boosts trust among employers, academic institutions, and students. Employers can easily verify a candidate's qualifications without contacting universities, streamlining the hiring process and ensuring credibility.

6.10. Sustainability and Paperless Academic Records

Blockchain eliminates the need for paper-based certificates, reducing environmental impact. Since all academic records are stored digitally, institutions can transition to a fully paperless system, making credential verification more sustainable and eco-friendly.

7. CHALLENGES IN BLOCKCHAIN BASED ACADEMIC CREDENTIAL VERIFICATION

While blockchain-based credential verification systems offer numerous advantages, they also come with challenges and limitations that must be addressed for effective implementation. Below are some of the key challenges:

7.1. Scalability Issues

Public blockchains often experience scalability constraints, leading to slow transaction processing speeds and high gas fees. This can become a bottleneck for large-scale credential verification, especially when handling massive volumes of student records and verification requests simultaneously.

7.2. Regulatory and Legal Compliance

Blockchain regulations vary across countries, making it challenging for educational institutions to ensure compliance with data privacy laws such as **GDPR** and **FERPA**. Additionally, legal recognition of blockchain-issued credentials is still evolving, leading to uncertainty in their acceptance by regulatory bodies and employers.

7.3. Lack of User Awareness and Adoption

Many academic institutions, employers, and students are not fully familiar with blockchain technology, leading to hesitation in adoption. Educational institutions may lack the technical expertise to integrate blockchain-based credential verification into their existing systems, while employers may still rely on traditional verification methods.

7.4. Dependence on Internet Connectivity

Since blockchain-based credential verification relies on internet access, users in regions with poor connectivity may face difficulties in accessing and managing their digital credentials. This can be a barrier for students and professionals in remote or underserved areas.

7.5. Challenges in Credential Transferability

While blockchain makes credential transfers easier, challenges can arise when transferring records between different educational institutions or across borders. Some institutions may not yet recognize blockchain-based credentials, causing inconsistencies in acceptance and interoperability issues between different blockchain networks.

8. CONCLUSION

This report explores the integration of blockchain technology into academic credential verification, addressing key challenges in traditional systems. It highlights inefficiencies in paper-based and centralized digital records, such as fraud risks, manual verification delays, and lack of transparency. By leveraging blockchain's immutability and decentralization, the proposed system enhances security and trust in academic credential verification. The use of smart contracts automates credential issuance, verification, and revocation, reducing dependency on intermediaries and ensuring seamless authentication processes.

The blockchain-based credential verification system provides a structured approach to securely managing academic records. Educational institutions can issue and register credentials, while students and employers can verify their authenticity instantly. The system ensures that revoked or expired credentials are automatically invalidated, preventing fraud and misuse. This transition to a blockchain-powered model aligns with global efforts to reduce reliance on paper-based documentation, enhance student mobility, and promote secure, decentralized credential management.

8.1. Future Outlook for Enhancements

To further optimize the system, artificial intelligence (AI) can be integrated for fraud detection by identifying suspicious credentialing patterns and inconsistencies. AI-driven analytics can also enhance data insights for institutions and employers, helping them verify academic achievements more efficiently. Additionally, AI-powered chatbots can provide instant assistance to students, universities, and employers in navigating the credential verification process.

The integration of Decentralized Identity (DID) solutions could enhance privacy and user authentication, ensuring that only verified individuals can access and share their credentials. This would enable students to maintain control over their academic records while preventing unauthorized modifications or misuse.

For global adoption, interoperability with multiple blockchain networks can be explored to enable seamless cross-border credential verification. This would benefit students applying for higher education or employment in different countries, as their academic records could be instantly verified across institutions and organizations worldwide.

To address scalability challenges, Layer 2 blockchain solutions can be implemented to reduce costs and improve transaction speeds, making the system practical for large-scale institutional use. Additionally, a hybrid blockchain model—combining public and private blockchains—can optimize cost-efficiency while maintaining security and decentralization.

By continuously improving the system with these advancements, blockchain-based academic credential verification can evolve into a secure, efficient, and globally accepted solution for modern education and employment sectors.

9. SDG’s ADDRESSED

The blockchain-based academic credential verification system aligns with several United Nations Sustainable Development Goals (SDGs) by enhancing transparency, reducing fraud, promoting digital transformation, and ensuring secure and verifiable academic records. Below are the key SDGs addressed and their justifications:

SDG 4: Quality Education

The system ensures equitable access to verified academic credentials, enabling students worldwide to securely store and share their educational achievements. By reducing fraudulent certifications and ensuring the integrity of qualifications, blockchain technology enhances trust in academic records and supports lifelong learning opportunities.

SDG 9: Industry, Innovation, and Infrastructure

The implementation of blockchain in credential verification fosters technological innovation and digital transformation in education. By replacing manual and paper-based verification processes with decentralized, tamper-proof records, institutions and employers can efficiently authenticate credentials and streamline admissions and hiring. The automation of verification through smart contracts reduces delays and enhances infrastructure reliability in the education sector.

SDG 16: Peace, Justice, and Strong Institutions

Blockchain-based credential verification prevents fraud, document forgery, and identity misrepresentation by providing immutable academic records. It promotes transparent and verifiable educational qualifications, ensuring that only authentic credentials are recognized. This fosters trust among institutions, students, and employers, strengthening global academic and professional systems.

SDG 13: Climate Action

Digitizing academic credentials eliminates paper-based certificates and transcripts, reducing deforestation and the carbon footprint associated with printing and physical document transportation. The automation of verification processes also reduces administrative burdens, minimizing energy consumption linked to traditional verification methods.

By integrating blockchain technology, the academic credential verification system contributes to a secure, transparent, and sustainable ecosystem that promotes trust in education, fosters innovation, and reduces environmental impact.

10. REFERENCES

[1] Intellinet System, "Benefits of Employing Online Academic Credential Verification Solutions," Available at:
https://www.intellinetsystem.com/blogs/benefits-of-employing-online-warrantymanagement-solution

[2] Intellinet System,"Blockchain for Academic Credential Verification,"Available at:
https://www.intellinetsystem.com/blogs/digital-warranty-management-blockchain

[3] ResearchGate, "Blockchain-Based NFT Credential Verification System: A Software Implementation,"Available at:
https://www.researchgate.net/publication/387261105_BlockchainBased_NFT_Warranty_System_A_Software_Implementation

[4] IJCRT, "A Study on Blockchain-Based Academic Verification Systems," Available at:
https://www.ijcrt.org/papers/IJCRT2406197.pdf

11. APPENDIX A

https://drive.google.com/drive/folders/1NI4GfK4bjohnAxsCFUN1ANh6_-PUkQZa