

# Blockchain in Higher Education: Advancing Security, Verification, and Trust in Academic Credentials

Kennedy C. Cuya<sup>1</sup>, Thelma D. Palaoag<sup>2</sup>

<sup>1</sup>*College of Engineering and Computational Science, Partido State University, Camarines Sur, Philippines*

<sup>2</sup>*College of Information Technology and Computer Science, University of the Cordilleras, Baguio City, Philippines*

*Email: kennedy.cuya@parsu.edu.ph*

The integration of blockchain technology in higher education presents a transformative approach to enhancing the security, verification, and trust of academic credentials. This paper investigates the application of blockchain to address the persistent issues of academic document forgery and inefficiencies in the verification process. By leveraging blockchain's immutable and decentralized nature, the proposed system ensures the authenticity and integrity of academic records, significantly reducing the risk of fraud. The study highlights the system's features, including enhanced security, efficiency, accessibility, and transparency, making it a universal solution for academic credential management. Detailed case studies and implementations demonstrate the practicality and effectiveness of this technology in real-world scenarios. While challenges such as the need for technological adoption and digital infrastructure remain, the potential benefits underscore blockchain's strategic role in revolutionizing academic record management, fostering a more secure, efficient, and trustworthy academic environment. This research contributes valuable insights into the deployment of blockchain in education, offering a robust framework for future advancements in secure document management.

**Keywords:** Blockchain technology, credential management, digital certificates, verification process.

## 1. Introduction

Academic credentials are an important part of academic integrity, and fraud-proofing them also helps in maintaining public confidence in higher education. With the changing paradigms of the education world, it is increasingly hard for institutions to safeguard academic credentials from counterfeit and forgery. Dissemination of false academic records is the primary. The blockchain technology is shown as a vision of the new solution for these problems, presenting possibilities that were never seen before to assure the security,

verifiability, and credibility of academic credentials.

The technology is a decentralized digital ledger technology that earned notoriety for being ultra-secure, unchangeable, and transparent. Blockchain technology, by design, can well serve as a perfect platform for school record management since it allows a verifiable and unchangeable system. In higher education, blockchain technology goes beyond mere digital storage to revolutionize credential verification procedures and cut down on administrative costs, hence enhancing academic record management.

This paper considers the incorporation of blockchain technology into higher education, with a special focus on how the system might enhance the security measures related to academic credentials. We can learn the characteristics of the architecture and functionalities of a blockchain that make it applicable to these kinds of uses: for instance, the possibility of automation and securing of transactions through smart contracts, as well as the possibility of building an international, interoperable ledger that both employers and universities can access, with recent graduates. This paper shows a deep analysis of case studies and existing implementations that have been and are currently in use, giving proper understanding of how blockchain technology can be applied to foster a more secure, efficient, and trustworthy academic environment.

But, of course, as we consider these options, it becomes evident that blockchain is a strategic tool towards addressing not just another new technology but some of the major challenges of higher education today. Blockchain technology keeps the individual accomplishments, along with the scholarly value and repute of institutions of learning around the globe, safe and intact through assurance on the integrity and safety of academic credentials.

## **2. Related Literature**

The literature on blockchain technology in higher education, particularly in the management and verification of academic credentials, presents a vibrant array of research efforts focused on enhancing security, verification processes, and trust among stakeholders. A significant portion of the research focuses on the deployment of blockchain for securing and verifying academic records. For instance, the paper "ACC: Blockchain Based Trusted Management of Academic Credentials"[1] discusses a blockchain-based system that provides a decentralized approach to manage and verify academic credentials efficiently, ensuring that data is unalterable and securely accessible to authorized entities only. The paper of Arndt, et.al [2] elaborates on the use of blockchain as a decentralized ledger to enhance the verification process of educational certificates. It emphasizes the need for a system that can reliably verify the authenticity of academic qualifications in a manner that is both secure and cost-effective. For educational certification system framework based on blockchain technology, researchers proposes a framework that uses blockchain to record and transfer academic credits and certificates digitally[3]. It highlights blockchain's ability to ensure transparency and trust among all participants in the educational ecosystem, including universities, accreditation bodies, and employers. Similarly, another paper reviews the application of blockchain technology to create a more transparent, reliable, and secure environment for verifying educational credentials. It underscores blockchain's role in reducing fraud and

increasing the efficiency of credential verification processes.

### Traditional Certification Problems

Institutions of higher education are increasingly grappling with the challenges of academic document forgery, fraud, and academic dishonesty. These issues compromise the integrity of academic credentials and highlight systemic vulnerabilities within the certification processes. The following analysis explores traditional certification problems in higher education, drawing from recent studies to elucidate the causes, manifestations, and possible solutions to these problems.

### Certification Challenges and Academic Integrity Violations

#### Credential Fraud

The demand for higher education credentials, coupled with high unemployment and the desire for social recognition, fuels the proliferation of credential fraud[4]. Institutions often face challenges due to the presence of degree mills, forgery, and corrupt officials, which contribute significantly to the increase in fraudulent academic and professional awards.

#### Vulnerability to Forgery and Manipulation

Educational certificates are crucial for verifying an individual's qualifications but are often susceptible to forgery and manipulation[5]. Traditional methods of verifying the authenticity and integrity of these certificates have proven inadequate in curbing fraud. This inefficiency fosters an environment where fraudulent activities can flourish, compromising the credibility of academic credentials.[5]

#### Inefficiencies in the Verification Process

The traditional process of verifying educational and professional certificates is often cumbersome and time-consuming. This not only delays career progressions but also allows for the proliferation of educational scams, as manual verification is more susceptible to human error and deceit.[6]

#### Challenges with Paper-Based Documentation

The reliance on paper-based degrees and certificates adds to the risk of damage or loss, and it makes forgery easier. Paper documents are difficult to verify quickly and accurately, which can lead to significant delays and potential errors in the verification process[7].

#### Proposed Work

The purpose of this paper is to examine the feasibility of implementing an effective anti-forgery mechanism for academic documents, including but not limited to mark sheets, transcripts, diplomas, and related certificates. By ensuring the authenticity of academic documents, reducing the number of instances in which certificates are counterfeited, and saving time and financial resources for all parties involved in document verification, the goal is to achieve the desired results.

The proposed solutions center on three different roles or entities: the Issuer, the Verifier, and the Student.

- The authority that is responsible for creating and issuing the electronic version of the certificate is known as the issuer. For example, a university that is responsible for issuing graduating certificates.
- A potential employer or any other individual who wishes to verify the authenticity of the certificate that the student has provided is the verifier. For example, a potential employer conducting a background check is an example of a verifier.
- Lastly, the student is the recipient of the certificate, and he is the only person who can view the documents that have been issued to him.

The purpose of this project is to develop an effective anti-forgery mechanism for academic correspondence. A combination of blockchain technology, the Internet Protocol File System (IPFS), and hash functions can be utilized to guarantee the authenticity of the certificate. This will result in a decrease in the number of certificates that are counterfeited, as well as a reduction in the amount of time and financial resources required for document verification activities.

### System Features

In the rapidly evolving educational landscape, the verification and management of academic documents remain critical yet challenging endeavors. Institutions worldwide grapple with the dual demands of ensuring document security and verification while maintaining accessibility and efficiency. This paper proposes a revolutionary platform designed to transform the management of academic credentials through the integration of blockchain technology, the InterPlanetary File System (IPFS), and cryptographic hash functions. This comprehensive solution addresses the myriad challenges faced by educational institutions, students, and employers alike by ensuring the authenticity, immutability, and easy accessibility of academic records. This incorporates several groundbreaking features that leverage advanced technologies to transform the way academic documents are managed and verified. Here's a detailed discussion on each feature of the system:

**Security:** By using blockchain, IPFS, and hash functions, the application provides a highly secure platform for storing and verifying academic documents. The blockchain is tamper-proof and immutable, ensuring that the data stored on it cannot be modified or deleted. The use of hash functions ensures that any modification to the document will be detected, making it difficult for counterfeit certificates to be created.

**Efficiency:** it streamlines the process of verifying academic documents[8], saving time[9] and resources[10] for all parties involved. Verifiers can easily access the certificates and compare the hash values, eliminating the need for manual verification[11].

**Accessibility:** the application makes it easy for students to access and share their academic documents. The use of IPFS allows for quick and easy access to the documents[11], while the Universally Unique Identifier (UUID) ensures that the documents are easily identifiable and verifiable.

**Transparency:** The use of blockchain ensures transparency and accountability in the issuance and verification of academic documents.[12] All data related to the certificate and the IPFS link are stored on the blockchain, providing a transparent and auditable record of the entire process.

**Universality:** This can be used by any educational institution, making it a universal solution for ensuring the authenticity of academic documents[13]. The platform can also be used by potential employers, government agencies, or any organization that needs to verify the authenticity of academic documents.

Architecture

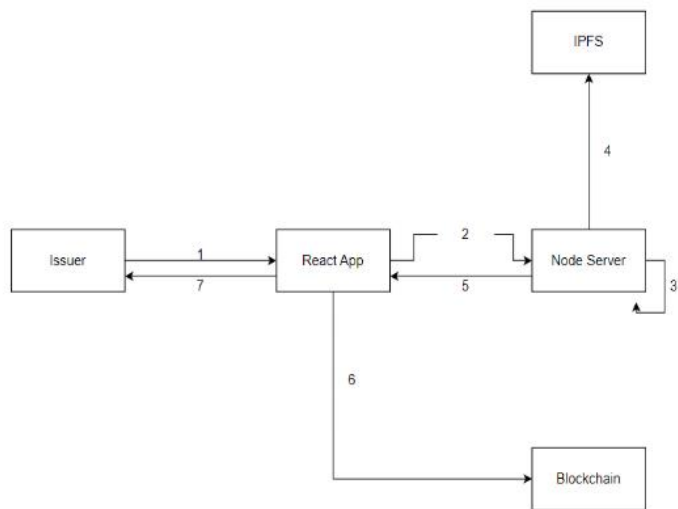


Figure 1 Issuer workflow process

The workflow depicted in the diagram illustrates a secure and decentralized process for managing documents, initiated by an Issuer who interacts with a React application. The Issuer begins the process by submitting data or a request to the React application, which may involve sending a document or credential for recording or verification. Upon receiving this data, the React application processes and forwards it to a Node server, potentially performing preliminary validations or formatting. From the Node server, there are multiple interactions: it records transactions or retrieves data from the blockchain, ensuring the data becomes part of an immutable ledger. Concurrently, the Node server may upload the document or data to the IPFS to handle larger data files off-chain while maintaining their accessibility. After storing the data on IPFS, the Node server retrieves the IPFS hash or other relevant metadata, which is crucial for updating the blockchain with a pointer to the data's location. This IPFS hash or additional transaction data is then recorded on the blockchain by the Node server, which finalizes the data's immutability and ensures the document's existence and integrity are verifiable via the blockchain. The React app receives confirmation or the results of the blockchain transactions, which could include success messages, error notifications, or retrieval of requested information. This information is then relayed back to the Issuer,

completing the process cycle.

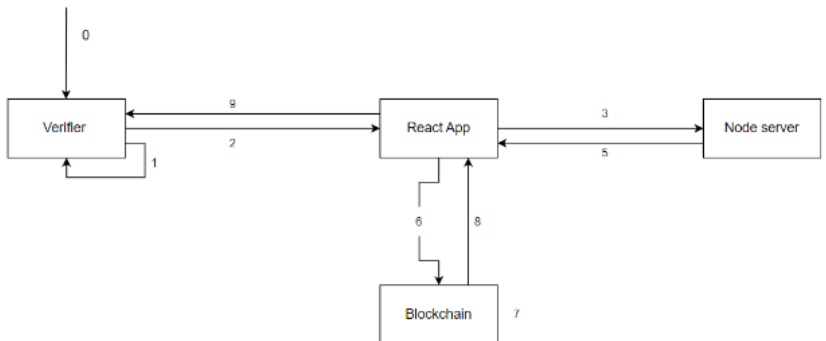


Figure 2 Verifier workflow process

The Fig 2. outlines the verifier workflow process within a system utilizing a React application, a Node server, and a blockchain. This workflow demonstrates how a verifier interacts with the system to verify data or transactions. Here's the workflow explained in paragraph form:

The process starts when the verifier initiates a query or verification request (0). This request is sent to a React application, which acts as the front-end interface for the verifier to interact with the system (1). The React application handles the request and then passes it on to the Node server (2). This server functions as the intermediary, managing backend operations like retrieving data and executing logic. When the data is received from the React application, the Node server seamlessly interacts with the blockchain to retrieve or verify the required information (3). Similar to a data scientist, the blockchain, renowned for its unchangeable and reliable storage, handles the request and returns the necessary data or verification confirmation to the Node server (4). The information is sent back to the React application by the Node server (5), and then the data is processed and presented to the verifier in a format that is easy to understand (6). During this process, there might be ongoing communication between the React application and the Node server to adjust or updates to the request based on the verifier's input or system responses (7, 8). After the verification process is finished and the verifier has obtained the necessary information or confirmation, the React application will show the results (9). This could involve providing information about the verified transaction, the status of data integrity, or any other pertinent output based on the initial query from the verifier.

Use Case Diagrams

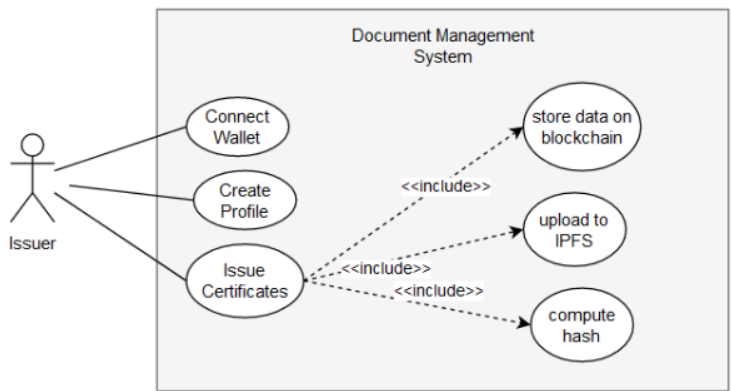


Figure 3 Use case for the Issuer

Fig.3 is a use case diagram that outlines a workflow where an issuer interacts with a document management system that utilizes blockchain technology and the IPFS. At first, the issuer links their digital wallet to verify their identity, which is necessary for managing transaction fees related to document operations. Subsequently, they proceed to establish or modify their profile in anticipation of issuing certificates. The primary purpose of the system is to issue certificates, which entails securely and permanently storing the document data on the blockchain. The system uploads large document files to IPFS, enabling decentralized and efficient data storage. At the same time, the system calculates a distinct hash value for each document when it is uploaded to IPFS and then records this hash value on the blockchain. This guarantees that although the document is stored efficiently off-chain, its integrity can always be confirmed by its hash stored on the blockchain, ensuring the document's genuineness and enduring nature. This dual-system approach effectively handles document security and accessibility, which is essential in environments where document integrity is of utmost importance.

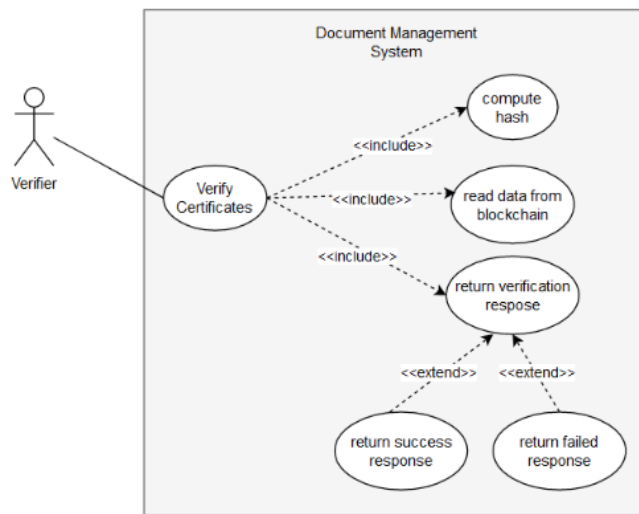


Figure 4 Use case for the Verifier

This use case diagram for the verification process of a document management system is presented in Fig. 4. In this respect, it is the verifier who has initiated a request to verify the certificates that will have the following activities conducted by the system: The system will compute the hash of the document to verify that it corresponds to the hash under which the document was initially processed. It retrieves the relevant data of the document from the blockchain, where the integrity and authenticity of the document are maintained. Afterwards, it collects the data and performs the hashing process, which is followed by the system release of the result of the verification process. A success response is sent back to the verifier in the event the computed hash and blockchain data agree to the authenticity of the document. It will only invalidate the response in the contrary, if any discrepancy is found with the data or the hash. It is done in such a way that the verifier has a clear, lucid outcome of verification based on the irrefutable record stored on the blockchain.

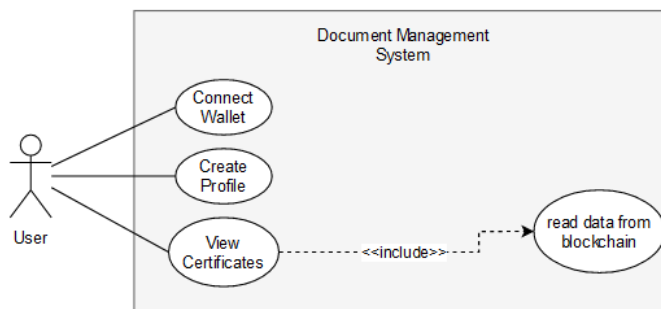


Figure 5 User's use case

Fig. 5 describes the potential ways a user would interact with a document management system. *Nanotechnology Perceptions* Vol. 20 No.S3 (2024)



system and highlights three important issues: first, a user signs in to the digital wallet to identify himself or herself through the secure and trusted mode of transaction on the system. Thereafter, a user can create or update their profile to manage personal information and preferences related to document management. The main core functionality that a user gets to access is the viewing of the certificates. This comes from the document data that is fetched from the system based on blockchain, on which the certificates are securely stored and maintained. Through this use of blockchain technology, data is immutable and verifiable to form a reliable source of truth for the documents the user will be able to view. This simplified workflow allows users to confidently handle and access their certificates in a secure manner, knowing that the integrity of the information is preserved.

### 3. Results and Discussion

The implementation of a blockchain-based certification system for issuing, verifying, and managing academic certificates has been illustrated through a series of user interface snapshots detailing the process from registration to verification. This section provides a detailed analysis of the results observed during the operation of this system, emphasizing its effectiveness in addressing traditional certification problems.

#### Registration Process

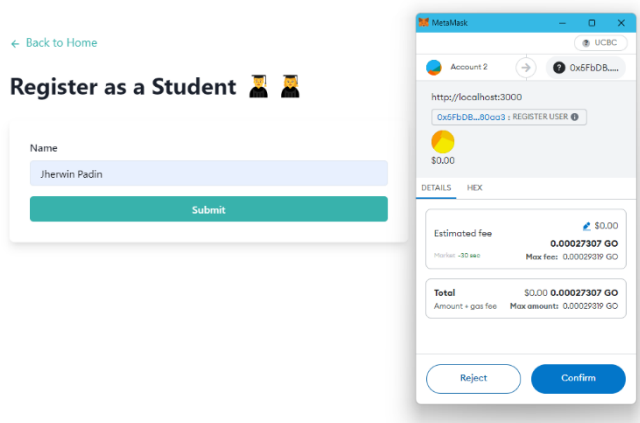


Figure 6 Student registration

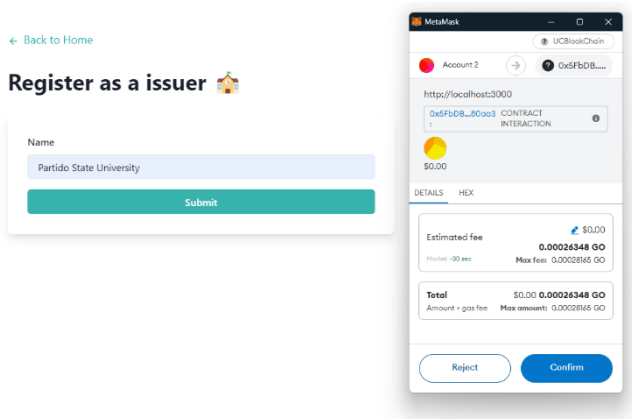


Figure 7 Issuer Registration

The system allows two types of users to register: students (Fig.6) and issuers (Fig.7) (e.g., educational institutions). The registration process is straightforward, requiring only the essential details such as the name for both students and issuers. This simplicity enhances user engagement and system accessibility. Upon registration, users are integrated into the blockchain network, establishing a secure and immutable record of their identity.

Issuance of Certificates

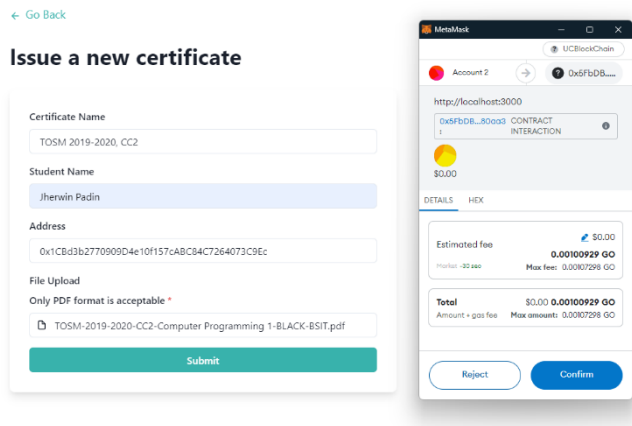


Figure 8 Issuing certificate or document

You have Issued 1 Certificates Issue New Certificate

NAME	UUID	ISSUED TO	LINK TO CERTIFICATE
TOSM 2019-2020, CC2	116a0b1-071d-4810-b244-380a92291579	0x1CBd3b277090D4e10f157aBC84C7264073C9Ec	<a href="#">View Certificate</a>

Figure 9 Certification details

Fig. 8 showcases certificates that are issued by registered educational institutions to students or clients. The issuer inputs details such as certificate name, student name, and a unique

address, along with the certificate file itself (only PDF format accepted). This process ensures that all issued certificates are recorded on the blockchain, providing a tamper-proof ledger entry that guarantees the integrity of the document. Fig. 9 shows that the system also assigns a unique identifier (UUID) to each certificate, further securing and distinguishing each document.

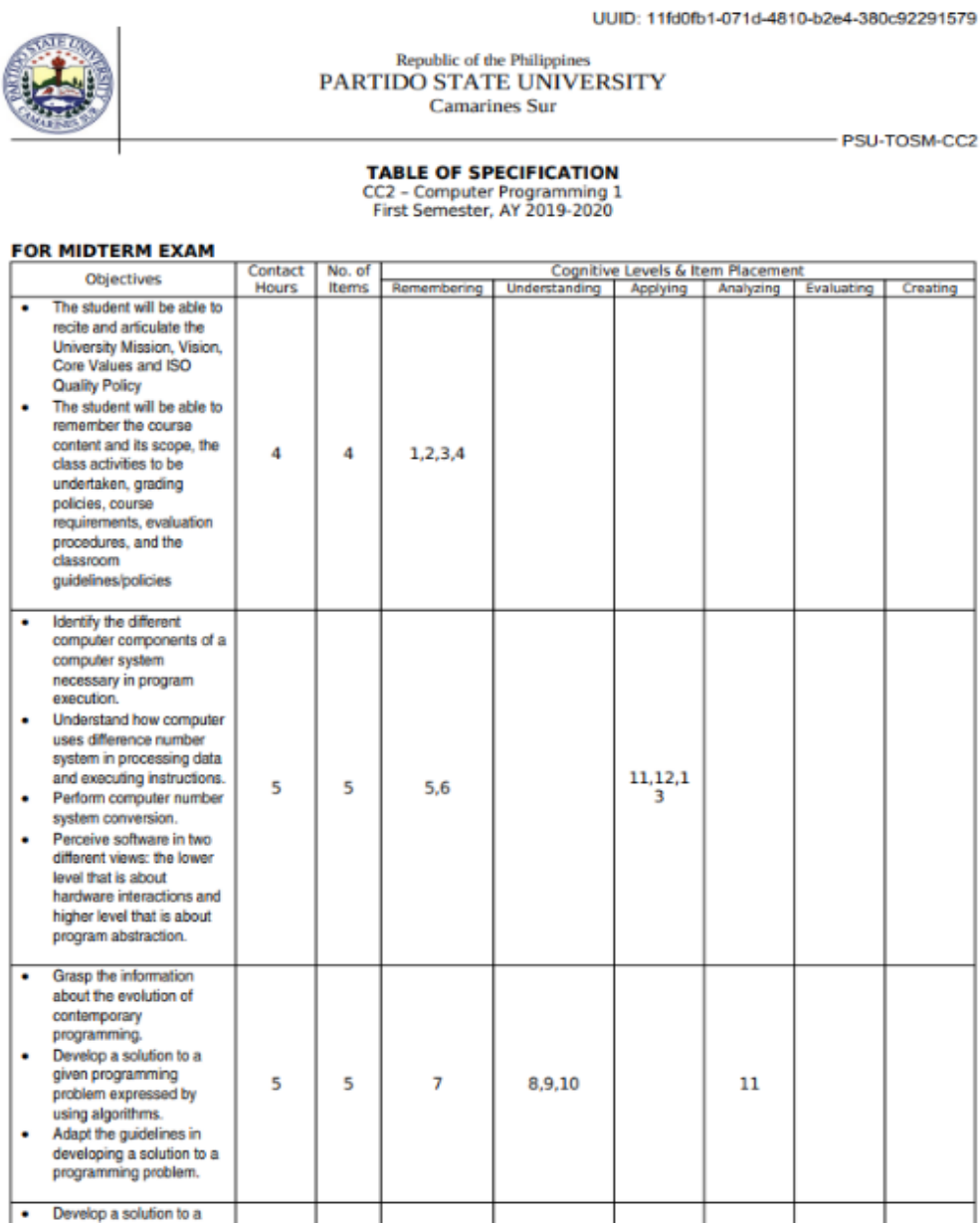


Figure 10 Sample certificate or document with UUID

## Verification of Certificates

[← Back to Home](#)

### Verify a document

Issuer Wallet Address

Student's Wallet Address

UUID

File Upload

Only PDF format is acceptable \*

**Submit**



 Document is Authentic 

Figure 11 Verification of documents

The verification process is a critical component of the system. To verify a certificate, the user must provide the issuer's wallet address, student's wallet address, UUID, and the certificate file (Fig.11). The system checks these inputs against the blockchain ledger to confirm the authenticity of the certificate. This process eliminates the common issue of certificate forgery and fraud found in traditional systems, as the blockchain's immutable nature ensures that all entries are permanent and unalterable once confirmed. The user interface provides clear, concise feedback at each step. For instance, upon successful verification, the system displays a confirmation message stating, "Document is Authentic." This immediate feedback is crucial for user satisfaction and trust in the system. The interface design is user-friendly, encouraging wider adoption and easing the transition for users from traditional paper-based or less secure digital systems.

### Practical Implications

Implementing this blockchain-based system addresses several critical issues in traditional academic certification processes:

- **Reduction in Fraud:** The immutability and encryption inherent in blockchain technology significantly reduce the risk of fraud and certificate forgery.
- **Efficiency:** The system automates the verification process, reducing the time and resources required to verify academic documents.
- **Transparency and Trust:** Blockchain provides a transparent system where all transactions are visible to authorized users, thereby increasing trust among students, educational institutions, and potential employers.

### Challenges and Limitations

While the system demonstrates considerable advantages, challenges such as the need for

*Nanotechnology Perceptions* Vol. 20 No.S3 (2024)

widespread technological adoption and understanding of blockchain among users persist. Additionally, the system's reliance on digital infrastructure means that users without reliable internet access or technological tools may find it difficult to participate.

#### 4. Conclusion

The blockchain-based certification system successfully demonstrates an innovative approach to managing academic documents. By leveraging blockchain technology, the system addresses the vulnerabilities of traditional certification methods, offering a more secure, efficient, and reliable solution. This case study provides a valuable model for future implementations in other sectors requiring secure document management and verification.

Integrating blockchain technology and the IPFS in the document management system offers a strong solution for securely managing, verifying, and accessing academic and professional certificates. The system utilizes the inherent unchangeability of blockchain to guarantee the preservation of the integrity and genuineness of each document, while IPFS manages the storage of large data files, addressing issues of scalability and efficiency. The workflow diagrams depict the intuitive interactions that enable issuers to effortlessly generate, store, and authenticate certificates, while also providing verifiers and users with a seamless and dependable means to validate and access these documents. Implementing this system has the potential to greatly improve the reliability and effectiveness of managing academic and professional credentials on a global scale. The system's automation of crucial processes and guarantee of data integrity alleviate administrative burdens and mitigate potential errors, rendering it indispensable for educational institutions, employers, and individuals alike. Potential future advancements could concentrate on enhancing the system's functionalities to encompass a wider range of interactive features and diverse document formats, thereby potentially revolutionizing document management across multiple industries. In summary, the document management system exemplifies the potential of integrating blockchain and IPFS technologies, establishing a fresh benchmark for the management and authentication of digital documents in an ever more digitalized society.

#### References

1. M. Suman Reza, S. Biswas, A. Alghamdi, M. Alrizq, A. Kumar Bairagi, and M. Masud, "ACC: Blockchain Based Trusted Management of Academic Credentials," 2021.
2. T. Arndt, A. Guercio, and Y. Chae, "An Evaluation of Security in Blockchain-based Sharing of Student Records in Higher Education," *International Journal of Network Security & Its Applications*, vol. 14, no. 3, pp. 1–9, May 2022, doi: 10.5121/ijnsa.2022.14301.
3. O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain based framework for educational certificates verification," *Journal of Critical Reviews*, vol. 7, no. 3. Innovare Academics Sciences Pvt. Ltd, pp. 79–84, 2020. doi: 10.31838/jcr.07.03.13.
4. E. C. GARWE, "Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe," *Journal of Studies in Education*, vol. 5, no. 2, p. 119, Apr. 2015, doi: 10.5296/jse.v5i2.7456.
5. Smita Chaudhari, Soham Mohite, Shreya Kumbhakarn, Viren Rathod, and Sakshi Khairnar, "Blockchain based solution for academic certificate management system using smart contract,"

- International Journal of Science and Research Archive, vol. 8, no. 1, pp. 291–197, Jan. 2023, doi: 10.30574/ijrsra.2023.8.1.0037.
6. A. Singh, S. Chauhan, and A. K. Goel, “Blockchain Based Verification of Educational and Professional Certificates,” in 2023 2nd International Conference on Computational Systems and Communication (ICCSC), IEEE, Mar. 2023, pp. 1–7. doi: 10.1109/ICCSC56913.2023.10143008.
  7. S. Wadhwani, “Certificate Verification and Counterfeit Detection using Blockchain,” Int J Res Appl Sci Eng Technol, vol. 11, no. 11, pp. 1288–1294, Nov. 2023, doi: 10.22214/ijraset.2023.56705.
  8. Y. Shakan, B. Kumalakov, G. Mutanov, Z. Mamykova, and Y. Kistaubayev, “Verification of University Student and Graduate Data using Blockchain Technology,” INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL, vol. 16, no. 5, Sep. 2021, doi: 10.15837/ijccc.2021.5.4266.
  9. N. Dlamini, S. Mthethwa, and G. Barbour, “Mitigating the Challenge of Hardcopy Document Forgery,” in 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), IEEE, Aug. 2018, pp. 1–6. doi: 10.1109/ICABCD.2018.8465401.
  10. H. Gaikwad, N. D’Souza, R. Gupta, and A. K. Tripathy, “A Blockchain-Based Verification System for Academic Certificates,” in 2021 International Conference on System, Computation, Automation and Networking (ICSCAN), IEEE, Jul. 2021, pp. 1–6. doi: 10.1109/ICSCAN53069.2021.9526377.
  11. S. Khaleelullah, S. T. Vangapalli, M. Gaddam, V. S. Hanumakonda, and U. K. Goud Gangapuram, “Verification of Academic Records Using Hyperledger Fabric and IPFS,” in 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), IEEE, Jun. 2023, pp. 210–217. doi: 10.1109/ICPCSN58827.2023.00040.
  12. C. Turcu, C. Turcu, and I. Chiuchișan, “Blockchain and its Potential in Education.”
  13. E. P. Fedorova and E. I. Skobleva, “Application of blockchain technology in higher education,” European Journal of Contemporary Education, vol. 9, no. 3, pp. 552–571, Sep. 2020, doi: 10.13187/ejced.2020.3.552.