Integration of AI with BlockChain towards Authentication of Testimonials and Transcripts In Academic Institutions

Anant Jain[1][0009−0000−2859−8911], Gauranshi Gupta[1][0009−0001−9918−3120], and Rahul Johari[⋆1][0000−0002−7675−8550],

Deo Prakash Vidyarthi[3][0000−0003−4151−0552]

[1] SWINGER : **S**ecurity, **W**ireless, **I**oT **N**etwork **G**roup of **E**ngineering and **R**esearch, University School of Automation and Robotics(USAR), Guru Gobind Singh Indraprastha University, Delhi, India
[2] School of Computer and Systems Sciences, Parallel and Distributed System Lab JNU, Delhi, India

Abstract. This research paper investigates the fusion of Artificial Intelligence (AI) and BlockChain technologies to enhance the authentication of testimonials and transcripts in a Certificate Verification System. The motive behind this study was addressing the limitations of traditional certification processes, necessitating a shift toward more secure, transparent, and efficient methods. The proposed research approach utilzes Artificial Intelligence for candidate verification, via facial recognition and Optical Character Recognition (OCR). Afterwards, digital certificates are generated and securely stored on the BlockChain, using smart contracts for transparency. The result of AI and BlockChain provides an efficient verification process that ensures security and efficiency by verifying candidate credentials. Verified certificates are provided to recruiters or receiving parties, that shows the effectiveness of this proposed approach in certificate authentication system. This system not only ensures the security of candidate credentials but also enhances the verification experience for the receiving parties.

Keywords: Machine Learning · BlockChain · Data Science · Smart Contracts · Artificial Intelligence

1 Introduction

In today's world of emerging technology, especially the use of AI and Blockchain has provided several innovative practical ideas . This research is one of this kind of idea whose objective is to improve the certificate authentication system in academic institutions and reduce frauds which happens to poor verification process and centralized storage system.

⋆ corresponding author

1.1 Authentication using BlockChain

Blockchain can be understood as an immutable ledger maintaining the history of transactions using chain of blocks that are connected by the hash of the previous block. Blockchain technology uses decentralized consensus which means that no single entity has control over that data ensures trust and reduces the risk of fraud. A smart Contract can be understood as the lines of code written in programming languages like Solidity which execute automatically when desired conditions are met.

1.2 Authentication using Machine Learning

Machine learning techniques have a huge role in the generation and verification of testimonials and transcripts. Identity validation or facial recognition algorithms allows the system to analyze and verify individuals based on their unique facial features. Optical Character Recognition (OCR) technology enables the extraction of textual information from documents, which ensures accuracy in processing certificates. Validation and authenticity of certificates can be done by using these ML approaches that provides an additional layer of security to the overall BlockChain-based authentication framework.

1.3 The Synergy

The synergy of BlockChain and Artificial Intelligence in certificate system provides a secure and efficient process to generate, store and share certificates. Machine Learning technologies helps to verify the candidate by analysing facial features and documents using Face Recognition and OCR. After verifying the candidate, certificate is generated which is stored on the BlockChain in an immutable format and accessible with the help of unique hash.

2   Problem Statement

In today's world of certification generating and verification processes, scams and vulnerabilities are increasing very frequently, posing challenges to the reliability and integrity of digital certificates. The existing solutions for verifying the authenticity of certifications, such as testimonials and transcripts, lack a foolproof approach which leads to fraud and manipulation. Traditional verification methods are susceptible to document tampering, identity misrepresentation, and the inefficiency of manual validation processes.

Almost all the sectors are now relying on digital credentials, ranging from education to employment, there is a need for a robust and tamper proof system. The absence of a standardized and secure framework for certification authentication not only undermines the credibility of digital certificates but also introduces risks in recruitment and academic evaluation. This research aims to solve this issue by integrating security features of BlockChain with the analytical capabilities of Artificial Intelligence which provides a comprehensive solution to the uncertainty in the certification authentication process.

3   Literature Survey

In [1], the author explained about a BlockChain-based system to solve the issue of forged diplomas and transcripts. With the use of an automatic translation system along with Natural Language Processing, the system authenticates diplomas without using public certificates. Security is also enhanced by using hash algorithms and timestamp is used after the hashing is done. The system analyzes diploma authenticity using a four-point AI distribution method, that confirms the highest similarity in verified diplomas. This paper proposed NLP-based Blockchain Algorithm.

In [2], presents a comprehensive survey of BlockChain technology's potential to transform the educational system. It emphasizes how BlockChain can provide innovative, cost-effective learning methods, change teacher-student interactions, and issue immutable digital certificates, enhancing current certificate verification processes to be faster, more reliable, and independent of central authority. The survey compiles the relevant researches into a systematic literature review, covering significant contributions and focusing on developments from 2018 to 2022. The review offers recommendations for future research and practical applications, aiming to guide researchers, policymakers, and practitioners in this field.

In [3], this work explores the development of a BlockChain-based system to streamline the verification of academic credentials. Each year, millions of students transition to higher studies or the corporate world, necessitating the verification of their educational documents through a lengthy and cumbersome process. The proposed solution leverages BlockChain technology, particularly public BlockChains like Ethereum, along with Decentralized Applications (DApps) and Smart Contracts, to create a scalable and cost-effective method that drastically reduces verification time from days to seconds. The system includes a web application with a user-friendly front-end design for registration and verification requests. The backend comprises two key modules: an Optical Character Recognition (OCR) module to accurately extract details from certificates, and a BlockChain module to securely send and verify the data stored in the BlockChain.

In [4], the author describes that BlockChain technology offers a secure and transparent method for recording various types of data, such as educational certificates, marriage records, student records, and healthcare information. It enables the safe storage and maintenance of digital assets like professional, educational, and extracurricular certifications, crucial for assessing a student's achievements and showcasing their development and skills. This technology ensures data security and up-to-date maintenance at a low cost.

In [5], the literature review examines the potential of BlockChain Technology (BT) in enhancing trust, cooperation, identification, authenticity, and transparency. The review began with an analysis of peer-reviewed sources, supplemented by articles from various channels, to explore recent approaches, techniques, and trends in the use of BlockChain technology across sectors like banking, medical records, and education. The paper proposes a BlockChain-based dig-

ital certificate verification system, incorporating an owner authentication scheme and recording time and space data of students as blocks.

In [6], the authors explore the transformative impact of BlockChain technology on IT applications, emphasizing anti-forgery information, transaction verification, and smart contracts. They leverage these functionalities to develop the Vietnamese Educational Certification BlockChain (VECefblock), addressing counterfeit certificate issues in Vietnam. The study categorizes BlockChain research trends and outlines the principles for VECefblock development. Using Hyperledger Fabric on Amazon EC2 instance, they demonstrate the system's feasibility in a practical deployment environment, showcasing the potential of BlockChain in mitigating social issues and certificate management challenges in Vietnam.

In [7], the authors address the time-consuming process of academic certificate verification in employment scenarios. The paper highlights the delays in the issuance of offer letters due to the need for employers to authenticate certificates from issuing authorities, leading to prolonged selection processes. Proposing a solution, the authors advocate for BlockChain's verifiable distributed ledger and cryptographic mechanisms to counteract counterfeit academic certificates. The technology is presented as a common sharing platform for storing and accessing documents, aiming to minimize overall verification time and streamline the employment selection process.

In [8], the authors worked on the vulnerabilities of traditional paper and electronic certificates. It highlights the preservation, management difficulties and the issues of inconvenient verification, poor reliability to false verification. The paper proposed a decentralized certificate system proposal using BlockChain technology and smart contracts. It is specifically designed for college student's innovation and entrepreneurship competitions. This system employs smart contracts for functions like management, issuing verification, and many more functionalities.

In [9], the authors proposed BCert software which is a BlockChain-based system to increase the efficiency and security of academic documents storage, distribution, and verification. They used ethereum smart contracts and IPFS (InterPlanetary File System) for decentralized storage. BCert ensures a secure and distributed ledger of assets and transactions. All the information in the document was verified and stored on a public BlockChain by using hash functions. This ensures the validity of document through issuer's institution private key signatures.

4   Novelty

This paper provides the journey of a certificate, starting from its issuance by the certifying authority to its acceptance by the verifying party. The innovative AI + BlockChain architecture where AI technologies like Facial Recognition and OCR are used. The process begins with the collection of data followed by AI verification techniques to confirm the candidate's identity. Subsequently, the

certificates are stored on BlockChain using smart contract. This novel approach provides a reliable certificate storage solution that streamlines the accessibility of certificates by receiving parties.

5 Methodology Adopted

5.1 Proposed Approach

Summary of steps used in the process is provided below:

1. Data Collection and Preprocessing: All the personal and academic details of the student were provided to the system for issuing of certificate. Prepossessing techniques are applied to the collected data so that it can enter the next step of AI verification.

2. AI Verification: AI models are employed for identification and document verification. Facial recognition algorithms to validate the candidate's identity, Optical Character Recognition (OCR) for textual information extraction from documents.

3. Certificate Generation: After the identity of a candidate was verified a digital certificate was created with a unique identifier and digital signature to facilitate easy retrieval.

4. BlockChain Interaction: The digital certificates are securely stored on the BlockChain. This step utilises a smart contract to encapsulate the certificate details and generate a unique transaction ID for traceability. This step marks the ending of certificate issuing system as showcased in Fig 1.1 in section 4.1.

5. Confirmation and Notification: The candidates are informed about the successful certificate issuance. They are provided with the access to the BlockChain-stored certificate.

6. Certificate Verification: Recruiters or the receiving party have the ability to verify certificates during the hiring process. They initiate the verification process through a user interface using the unique identifier or public key.

7. BlockChain Verification: Smart contracts are executed to verify the authenticity of the certificate using the candidate's public key. This was done to ensure the certificate details match those stored on the BlockChain.

8. Verification Results: The verification results are communicated to the recruiter/receiving party. This step marks the ending of certificate issuing system as showcased in Fig 1.2 in section 4.1.

5.2   Flowchart

Certificate Issuing Process   **Certificate Accessing Process**

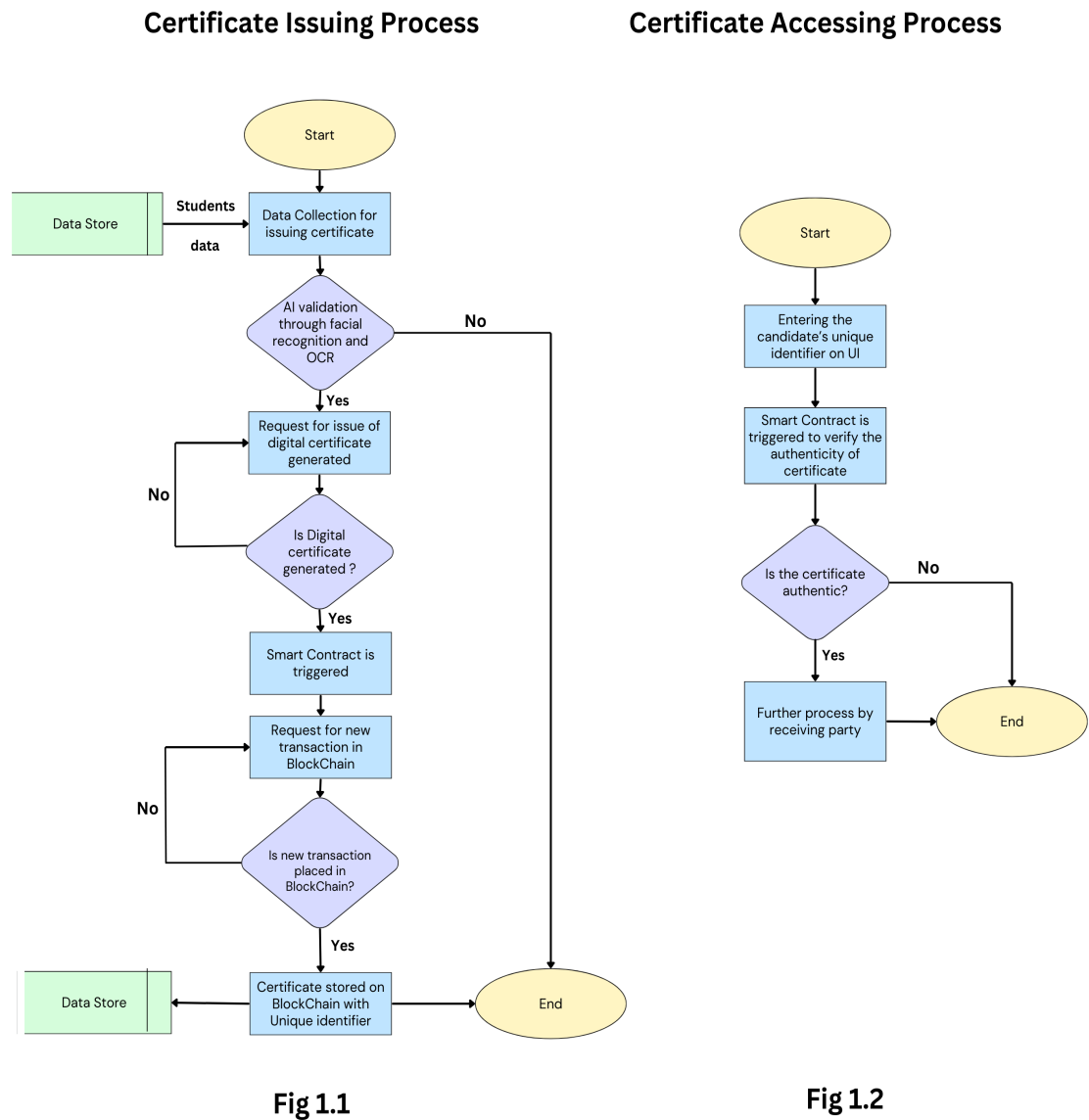**Fig 1.1**   **Fig 1.2**

Fig. 1: Fig 1.1: The entire process of issuing a certificate to a candidate. Fig 1.2: The entire process of accessing a candidate's certificate by the receiving company.

5.3   Algorithm Utilized

Below is the algorithm for Smart Contract functionalities which will be used to store and validate a certificate:

```
Data Structures:
    Certificate
        id (integer)
        candidateName (string)
        course (string)
        issueDate (string)
        valid (boolean)
        aiValidationHash (hash)

    AIValidation
        validated (boolean)
        validationHash (hash)

State Variables:
    admin (address)
    certificates (mapping: integer -> Certificate)
    aiValidations (mapping: string -> AIValidation)
    nextCertificateId (integer)
    issuers (mapping: address -> boolean)

Events:
    CertificateIssued (id)
    CertificateVerified (id, valid)
    AIValidationRecorded (candidateDetails, validationHash)
    IssuerAdded (issuer)
    IssuerRemoved (issuer)

Constructor:
    Set the contract creator as the admin

Functions:
    addIssuer (issuer: address)
        Only Admin
        Add a new issuer to the authorized issuers list
        Emit IssuerAdded event

    removeIssuer (issuer: address)
        Only Admin
        Remove an issuer from the authorized issuers list
        Emit IssuerRemoved event

    recordAIValidation (candidateDetails: string, validationHash:
         hash)
        Only Issuer
```

```
45          Record the AI validation result for the candidate
46          Emit AIValidationRecorded event
47
48      issueCertificate (candidateName: string, course: string,
            issueDate: string, aiValidationHash: hash)
49          Only Issuer
50          Check AI Validation (aiValidated modifier)
51          Create a new Certificate
52          Add the Certificate to the certificates mapping
53          Increment nextCertificateId
54          Emit CertificateIssued event
55
56      verifyCertificate (id: integer)
57          Return certificate details and validity status
58          Check if the certificate is valid
59
60      invalidateCertificate (id: integer)
61          Only Issuer
62          Invalidate a certificate if the sender is the issuer
63          Emit CertificateVerified event
```

5.4   Simulation Environment

Remix is an online integrated development environment (IDE) for Ethereum smart contract development. It provides a user-friendly platform for developers to write, deploy, and test the smart contracts on the Ethereum BlockChain. Below are the screenshots illustrating the implementation of various smart contract functionalities using Remix IDE:

5.5   Screenshots of IDE

In this smart contract, we begin by adding an authorized issuer using their public address. Following that, the AI hash will be recorded into the system. Then the issuer utilizes this hash to issue a certificate, ensuring a secure and verifiable certification process through BlockChain technology. If the AI hash is not recorded previously then the system will through an error and certificate will not be issued.
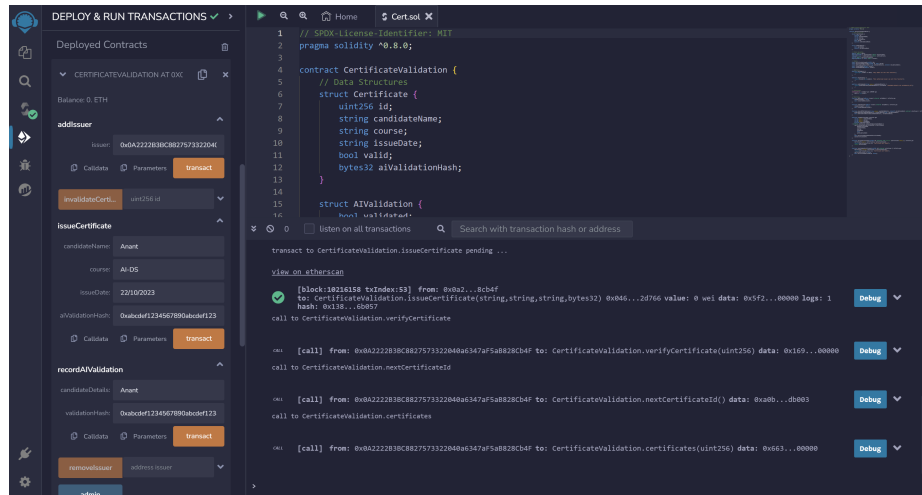
Fig. 2: Implementation of Issuing the certificate

The image displays a verified certificate issued to Anant for completing the AI-DS course. Issued on 22/10/2023, the certificate is validated through AI and deemed authentic. The AI validation hash ensures the certificate's integrity. Verified by authorized issuers, providing confidence in its legitimacy.
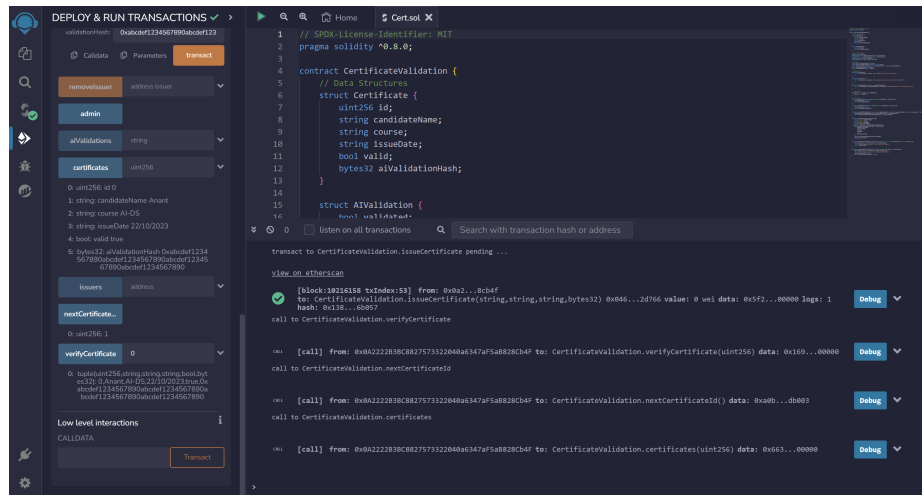

Fig. 3: Implementation of accessing the certificate

6   Results

The smart contract addressed 0x046528970B01f86abb082E87E043C5277162D766 has exhibited seamless functionality throughout the certification process. The system demonstrated its proficiency from the initial stage of adding the issuer to recording the AI hash, ensuring a secure and tamper-resistant foundation. The smart contract facilitated the generation of digital certificates with unique identifiers and digital signatures after successful AI verification, adhering to pre-defined criteria. The BlockChain interaction, managed through smart contracts, guaranteed the secure storage of certificates and the generation of unique transaction IDs for traceability.

The successful implementation of the smart contract validates the robustness of the proposed AI+BlockChain system in providing a secure and transparent solution for certificate issuance and verification.

7   Conclusion

In conclusion, the integration of Artificial Intelligence (AI) with BlockChain technology has demonstrated its effectiveness in establishing a secure, transparent, and efficient system for issuing, verifying, and retrieving certificates. This paper presents an end-to-end flow, starting with the issuance of certificates by academic institutions and culminating in the seamless access to certificates by recruiting parties through a unique hash. The integration of AI like facial recognition and Optical Character Recognition (OCR) techniques enhances the verification process, ensuring the accuracy and reliability of candidate credentials. This innovative system overcomes the challenges with traditional certificate authentication methods and contributes to a more trustworthy certification process by providing double verification process.

8   Future Work

Moving ahead, future work will focus on improvising the integration of the system with its AI components, working on AI algorithms for document verification and identity validation . Moreover, optimizing and expanding the functionalities of the smart contracts will be taken care along with proper auditing techniques, ensuring scalability and security. This research will explore potential collaborations with emerging technologies, contributing to the evolution of a well and improved AI+BlockChain certification ecosystem.

9   References

1. Kim, Seong-Kyu. 2022. "Blockchain Smart Contract to Prevent Forgery of Degree Certificates: Artificial Intelligence Consensus Algorithm" Electronics 11, no. 14: 2112. https://doi.org/10.3390/electronics11142112

2. Rustemi, Avni, Fisnik Dalipi, Vladimir Atanasovski, and Aleksandar Ris-
   teski. "A Systematic Literature Review on Blockchain-Based Systems for
   Academic Certificate Verification." IEEE Access (2023).
3. Gaikwad, Hrithik, Nevil D'Souza, Rajkumar Gupta, and Amiya Kumar Tri-
   pathy. "A blockchain-based verification system for academic certificates."
   In 2021 international conference on system, computation, automation and
   networking (ICSCAN), pp. 1-6. IEEE, 2021.
4. Pathak, Shivani, Vimal Gupta, Nitima Malsa, Ankush Ghosh, and R. N.
   Shaw. "Blockchain-based academic certificate verification system—a review."
   Advanced Computing and Intelligent Technologies: Proceedings of ICACIT
   2022 (2022): 527-539.
5. Kumutha, K., and S. Jayalakshmi. "The Impact of the Blockchain on Aca-
   demic Certificate Verification System-Review." EAI Endorsed Transactions
   on Energy Web 8, no. 36 (2021).
6. Nguyen, Binh Minh, Thanh-Chung Dao, and Ba-Lam Do. "Towards a blockchain-
   based certificate authentication system in Vietnam." PeerJ Computer Sci-
   ence 6 (2020): e266.
7. Kumar, K. Dinesh, P. Senthil, and DS Manoj Kumar. "Educational certifi-
   cate verification system using blockchain." international journal of scientific
   technology research 9, no. 3 (2020): 82-85.
8. Xie, Rui, Yuhui Wang, Mingzhou Tan, Wei Zhu, Zhongjie Yang, Jiaji Wu,
   and Gwanggil Jeon. "Ethereum-blockchain-based technology of decentralized
   smart contract certificate system." IEEE Internet of Things Magazine 3, no.
   2 (2020): 44-50.
9. Leka, Elva, and Besnik Selimi. "Bcert–a decentralized academic certificate
   system distribution using blockchain technology." International Journal on
   Information Technologies Security 12, no. 4 (2020).