Blockchain-based Academic Degrees Issuance and Attestation

Atta ur Rehman Khan, Raja Wasim Ahmad
College of Engineering and Information Technology
Ajman University
Ajman, United Arab Emirates.
dr@attaurrehman.com

***Abstract*— Academic degrees are usually issued in paper form and can be tempered easily. As the current systems lack transparency, immutability, and security, the verification of these degrees is a time-consuming and complicated process. In this paper, we present a blockchain-based solution for academic degrees issuance and verification in Pakistan.**

Keywords*— *blockchain; education; certificates; traceability; integrity.

I. INTRODUCTION

Higher education institutions and universities play a crucial role in production of skilled workforce. They help to make people qualify for more career opportunities by awarding them with certificates and degrees. These certificates and degrees are official documents, and enable recruitment companies to determine if the applicants possess the required knowledge and technical skills that are required for a particular role. These certificates/degrees are usually issued in paper form and are handled in either semi or non-computerized manner.

The current systems lack operational transparency, immutability, auditability, and security. Moroever, it is laborious, prone to frauds, and complicated. In the education industry, dishonesty, fraud, and bribery are prevalent problems that have a wide range of destructive and negative repercussions [1]. In the current system, the institutions/universities cannot only issue fake certificates/degrees, but they can also be attested from respective bodies with right resources. To counter these issues, there is a need for a new system that is not only fully computerized but also tranparent, immutable, and secure.

Over the past few years, blockchain technology has emerged as a viable solution to counter issues related to centralized systems, provide transparency, traceability, and security [2-4]. Considering the issues of the exisiting system and advantages of the blockchain technology, we present a blockchain-based solution for academic certificates issuance, attestation, and verification. The proposed system uses multiple smart contracts to record actions of the stateholders on immutable distributed ledger and ensures that all degrees are issued, attested, and verified as per defined rules. The issued degrees are digitally signed and files are stored on distributed storage system to avoid single point of failure and achieve scalability. As all records are stored on the blockchian, the verification of any certificate is not an issue. It is noteworthy, that our proposed system is inline with the exisiting workflow of operations, therefore, no major change is required by any stakeholder.

The rest of paper is organized as follows. Section II presents the related work, Section III presents the proposed system and its sequence diagrams, showing interactions between the stakeholders, Section IV presents the implementation details and algorithms, Section V presents the conclusions and future work.

II. RELATED WORK

In [5], the researchers present a privacy-aware solution for online credential management. This solution adopts a public blockchain model with other encryption systems for secure handling of the credentials. It is implemented and tested on fog-enabled cloud architecture to confirm its various

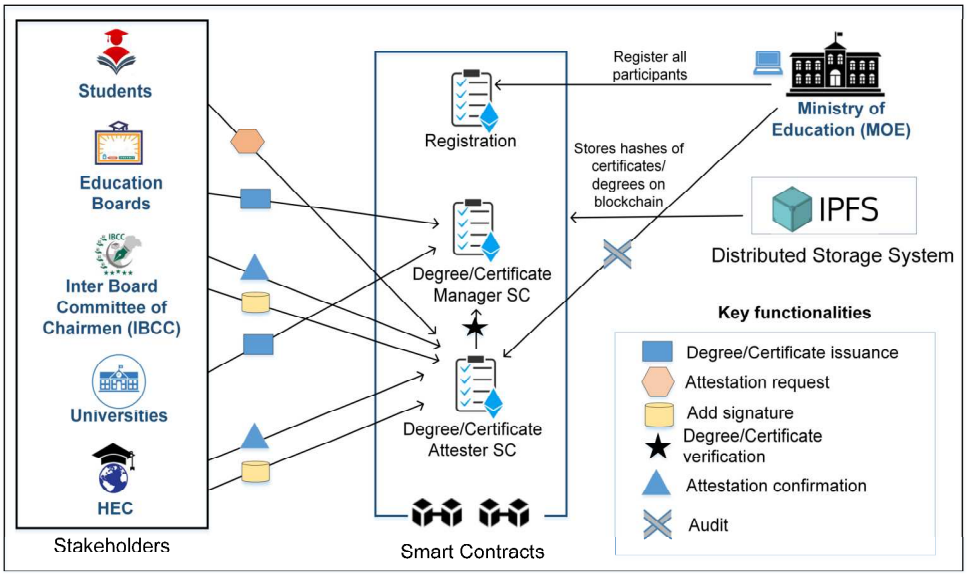

Fig.1. *Proposed blockchain-based degree verification system*

978-1-6654-8945-4/22/$31.00 ©2022 IEEE

performance and security parameters, such as privacy, latency, computational cost, and throughput.

In [1], the authors present HEDU-ledger, an educational blockchain ledger based on a private network architecture among the stakeholders. The proposed system provides attestation services and maintains a secure chain for tracing between peer nodes of the stakeholders. Moreover, it ensures the integrity of data and transactions. However, this system does not account for the issuance and authentication of certificates by educational boards and IBCCs.

In [6], the researchers present a blockchain-based solution for academic credential attestation. The researchers propose redesigning the process of academic credential attestation to save time, resources, and manpower. In addition, they suggest a method for collecting academic data to prevent fraud.

III. Proposed Solution

This section presents the high-level design of the proposed degree issuance and verification system. It highlights the main stakeholders (users), the blockchain layer (running smart contracts), and a distributed storage system (see Fig. 1). It also highlights the system users, their roles and operations, system components, and direction of data flow between various entities of the proposed blockchain-based system. The role and duties of users in the proposed system are discussed further in the following section.

A. System Participants and Components

This section highlights the responsibilities of each stakeholder involved in issuance and attestation of academic degrees in Pakistan. It also highlights the main system components that ensure that degrees issuance and attestation

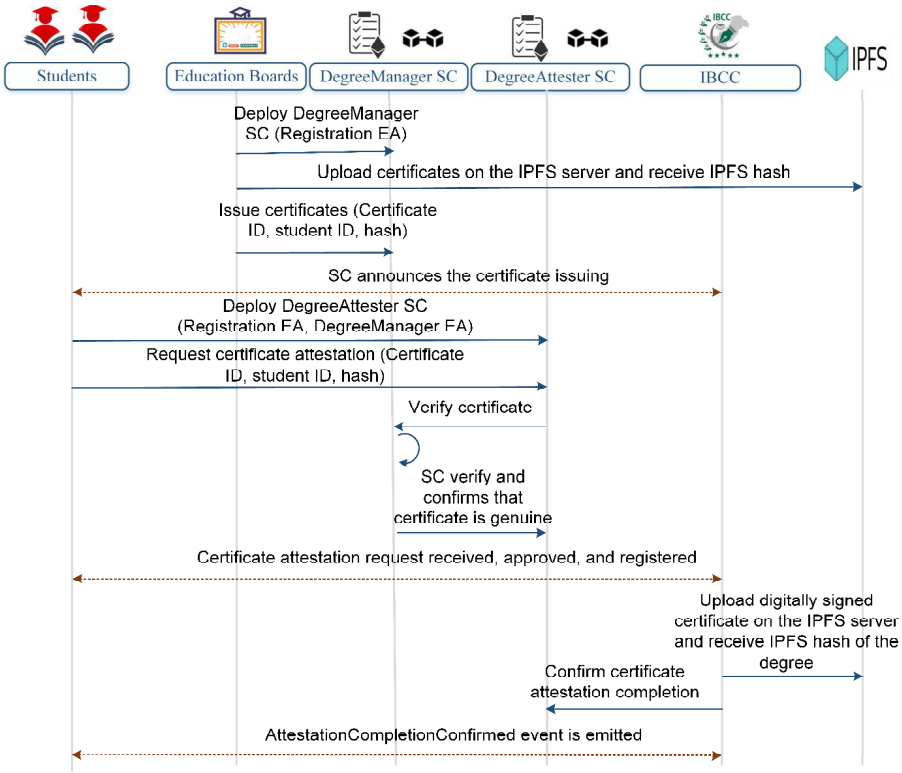

Fig.2. *Detailed sequence diagram illustrating the degrees recording on the blockchain and the attestation process*

In [7], the researchers present a solution for validation of academic credits and issuance of academic degree certificates. The solution is developed particularly for the Brazilian education system. In this solution, the higher education institutions are required to register students and their academic credits in a chain using Brazilian Public Key Infrastructure for identity management. This solution enables the decentralized issuance of degree certificates.

In [8], the researchers present a blockchain-based solution for credential verification to counter the fraud. This solution uses on-chain smart contracts for credential revocation and does not require the students or employers to manage digital identities. As per authors, the proposed system is more efficient than existing blockchain-based credential verification solutions.

related activities are executed in a secure, trusted, reliable, transparent, and verifiable manner. The main components and system participants of our proposed system are discussed as follows:

1) Students: Any person enrolled in a school, college, institute, or university is reffered to as a students. Upon completition of the accademic requirements, the students are issued certificates as a proof of achievement of the defined requirements.

2) Education Boards: There are multiple education boards in each state of Pakistan [9]. These boards are responsible for conducting exams and awarding Secondary School Certificates (SSC) and Higher Secondary School Certificates (HSSC) to the successful candidates. These boards are also responsible for attestation of the issued certificates [10].

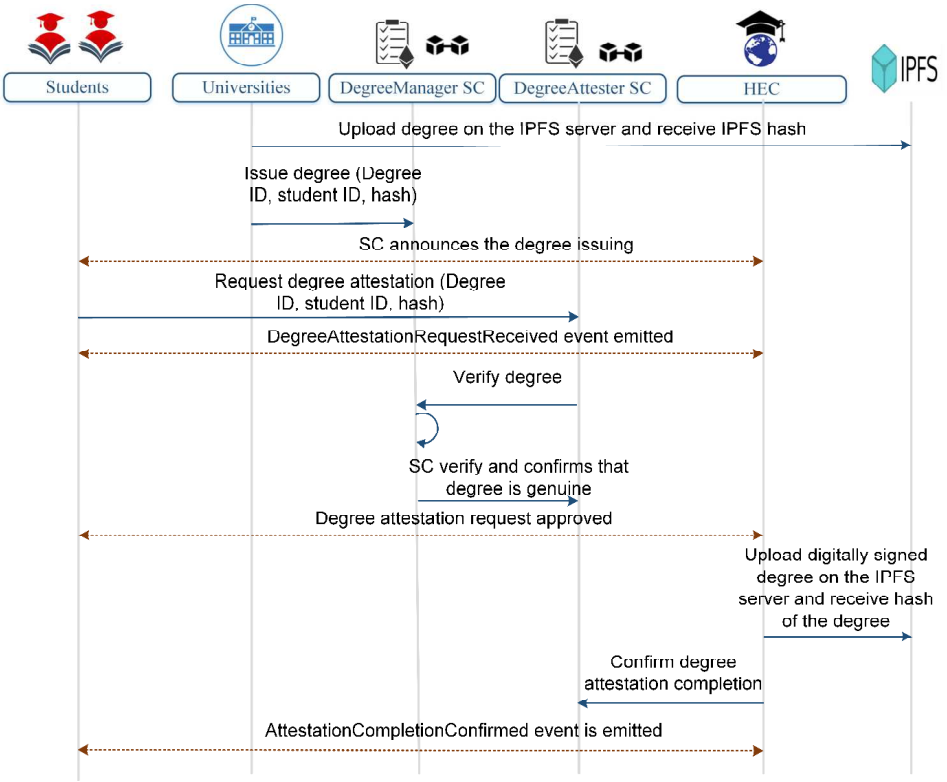

Fig.3. *Detailed sequence diagram illustrating the certificates recording on the blockchain and the attestation process*

3) Interboard Committee of Chairman (IBCC): IBCC shares information on all elements of Intermediate and Secondary Education among the members Boards to standardize academic evaluation and curriculum requirements [10]. It is also responsible for counter attesting the certificates issued by the education boards.

4) University: Univeriesites are high-level educational organization having degree awarding rights and are required to register with HEC [11].

5) Higher Education Commission (HEC): The HEC of Pakistan is an independent, autonomous, and constitutionally established institution of primary funding, overseeing, regulating, and accrediting the higher education efforts in Pakistan [12].

6) Ministry of Education (MoE): It is responsible for regulating the overall activites of the education sector. In Pakistan, MoE related activities are handled by the Ministry of Federal Education and Professional Training [13].

7) Smart Contracts: Smart contracts are computer programs that execute themselves and reduce the need for mediators while ensuring the administration of rules as agreed upon by the parties [14]. The smart contracts implement functions that are called when a certain event incurs relating to the issuance or attestation of the degrees. For this system, we propose multiple smart contracts, namely *Registration*, *Degree Manager SC*, and *Degree Attester SC*, to implement services related to degree certificates issuance, verification, and attestation.

8) Distributed Storage: Blockchain technology faces scalability issues, especially when massive files and data are to be stored on the blockchain [15]. Distributed storage solutions (e.g., IPFS[16]) allow stakeholders to store huge size files in a reliable and secure way without worrying about the scalability issues.

B. Sequence of Operations

This section presents the sequence diagrams for our proposed system. These diagrams show the function calls and events that occur on the blockchain when a function is called.

As shown in Fig.1, the MoE is responsible for registration of all participants discussed in the previous section. It is mandatory for the participants to be registered, otherwise, they will not be allowed to perform any action. The students will be registered on the system when they submit their applications for the SSC and HSCC examination. It is noteworthy, that students cannot register for HSCC examinations without attestation of their SSC certificate. Once the result of the exam is ready, the education board will issue certificates for the successful students. As shown in Fig. 2, whenever the education board issues a certificate, it will be stored on the IPFS and the related data (certificate ID, student ID, certificate hash) will be recorded on the blockchain. This will ensure integrity of the stored certificates and if any tempering attempt is made, it can be caught through blockchain because the hash of the original certificate is already recorded on the blockchain.

In universities case, the students will be registered after attestation of their HSCC certificate. Similar to the boards case, the universities will issue degree certificates to successful students only. These degree certificates will be stored on the IPFS and the related data (degree certificate ID, student ID, certificate hash) will be recorded on the blockchain (see Fig. 3). For this process, the system will use Algorithm 1. This algorithm performs some extra operations

as well, for instance, ensuring that the respective education board/university is registered, it is not in the list of the blacklisted universities, and the certificate hash is valid.

Fig. 2 shows a sequence diagram that highlights the users interaction with the system. Once certificate hash is recorded on the blockchain, the students can request for certificate attestation using student data (student ID, certificate ID, and certificate hash). Upon receiving the certificate attestation request, the system will verify the student record (student ID, certificate ID, certificate hash). Moreover, it will get the respective certificate from IPFS and then digitally sign the certificate and store it on the IPFS again.

The system will also get the hash of the digitally signed certificate and record it on the blockchain. In addition, it will emit a *AttestationCompletitionConfirmed* event to notify the relevant participants. The same process will be performed for attestation of degree certificates issued by the registered universities (see Fig. 3). For this process, the system will use Algorithm 2. This algorithm performs some extra operations, such as checking the student ID, institute ID, passing year, and degree certificate hash.

For digitally signing the certificates, the system use Algorithm 3. It is noteworthy that IBCC will have the authority to verify only the issued certificates, whereas HEC and MoE will have the authority to perform verification regarding authenticity of any type of certificate (SSC, HSSC, degree certificate).

Algorithm 1: Placing a degree attestation request.

Input: Student ID, Degree hash, Degree ID, Passing year, Institute ID
Output: Emit $DegreeAttestationRequestReceived$ and $DegreeAttestationRequestApproved$ Events
if *$StudentID$ is not registered* **then**
    The request is denied because the student ID is not verifiable.
end
else
    if *$InstituteID$ is recognizable* **then**
        Set request status to 'Request Sent'.
        Create an ID using Keccak 256 algorithm to identify the degree attestation request.
        Notify the relevant parties by emitting an event indicating the successful submission of a request for degree attestation using the Institute ID, Student ID, and Request ID.
    end
    else
        Display an error message and reset the smart contract to its initial state.
    end
    if *$Passingyear$ is valid AND $DegreeHash$ exists* **then**
        Set request status to 'Request Approved'.
        Notify the relevant parties by emitting an event indicating the request approval for degree attestation using the Institute ID, Student ID, Request ID, Request.status, and Degree hash.
    end
    else
        Display an error message and return the smart contract to its initial state.
    end
end

Algorithm 2: Issuance of a degree/certificate by universities/education boards.

Input: Student ID, IPFS hash, Degree/certificate ID
Output: Emit $DegreeCertificateIssued$ Event
if *$University/EducationBoards$ is not registered OR caller is not a $University/EducationBoards$* **then**
    The request is denied because the user ID is not verifiable.
end
else
    if *$University/EducationBoard$ does not belong to the list of black-listed universities category* **then**
        Store degree/certificate on IPFS server.
        Set status to "Degree/certificate Issued".
        Store IPFS hash of the degree/certificate on blockchain.
        Notify the relevant partitives by emitting an event ($DegreeCertificateIssued$) indicating the successful issuing of a degree/certificate using the Student ID, University ID, and Degree/Certificate Hash.
    end
    else
        Display an error message and reset the smart contract to its initial state.
    end
end

Algorithm 3: Digitally signing a degree/certificate by IBCC/HEC.

Input: Degree/certificate hash, Degree/certificate ID
Output: Emit $AttestationCompletionConfirmed$ Event
if *$IBCC/HEC$ is not registered OR caller is not $IBCC/HEC$* **then**
    The request is rejected due to an unverifiable address.
end
else
    if *Request.status ==Approved* **then**
        Digitally sign the degree/certificate and store it on IPFS server.
        Set status to "Degree/certificate Attested".
        Store IPFS hash of the degree/certificate on blockchain.
        Notify the relevant participants by emitting an event ($AttestationCompletionConfirmed$) reporting the successful signing a degree/certificate using the Student ID, HEC/IBCC ID, and Degree/Certificate Hash.
    end
    else
        Show an error message and put the smart contract back to the initial state.
    end
end

IV. Requirements and Implementation Guidelines

This section discusses the essential requirements and benefits of utilizing distributed technology for degree issuance and authentication. It also presents the guidelines for implementation of the proposed system.

A. Requirements

Data Accuracy: The stakeholders involved in the degree verification process rely on the blockchain's stored data.

Therefore, high accuracy and integrity is required by the stakeholders during the degree verification process. The immutability feature of blockchain ensures that data can not be altered by any party [17].

Data Privacy: Data privacy is another requirement of the academic degree issuance and verification process. As data breaches can result in information or identity theft, they may reduce users' trust in the system. To counter such issues, blockchain presents anonymous identity of the users to other participants.

Secure and Fast Data Sharing: Sharing of information between the parties involved in the degree issuance and verification process must be highly secure, swift, and reliable. In centralized systems, transaction execution is slow due to the presence of intermediaries. As a Peer-to-Peer (P2P) technology, blockchain enables the secure and rapid exchange of data between participants, since no intermediaries are required for verification and approval [18].

Storage: As the number of graduating students increases over time, so does the volume of data produced by academic institutions and degree verification entities. The increasing size of data can hinder the blockchain's performance; however, the blockchain stores data using IPFS to circumvent this issue [17].

B. Implementation Guidelines

The Ethereum private blockchain is a suitable candidate for implementing the proposed system. To validate transactions, the Ethereum blockchain employs the Proof-of-Work (PoW) consensus protocol. The certificate/degree issuance and verification smart contracts can be checked for vulnerabilities using the Oyente and SmartCheck tools [15]. Moreover, secure and bugs free smart contracts can be easily deployed and the system's users can be identified via unique Ethereum addresses. Event and transaction logs can be utilized to trace and validate the authenticity of academic certificates/degrees.

V. CONCLUSIONS AND FUTURE WORK

This paper presented design of a blockchain-based solution for academic certificates/degree issuance, attestation, and verification. The proposed system is capable of countering the problem of fake certificates in an effective, transparent, reliable, and secure manner. It will enable the IBCC and the HEC to perform quick and trusted verification. To resolve the scalability issues of the existing blockchain solutions, we used IPFS to store the certificates. Considering the overall system working of the proposed algorithms, we believe that the proposed system is viable and secure. It is noteworthy, the proposed system is generic and can be implemented for other environments considering the rules and regulations of a specific country. In the future work, we aim to deploy the proposed smart contracts on a blockchain and also integrate crypto payments for certificate verification requests.

REFERENCES

[1] A. Ayub Khan, A. A. Laghari, A. A. Shaikh, S. Bourouis, A. M. Mamlouk, and H. Alshazly, "Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission," Applied Sciences, vol. 11, no. 22, p. 10917, Nov. 2021.

[2] A. Rashid, A. Masood, and A. R. Khan, "Zone of trust: blockchain assisted IoT authentication to support cross-communication between bubbles of trusted IoTs," Cluster Computing, Mar. 2022.

[3] A. Rashid, A. Masood, and A. R. Khan, "RC-AAM: blockchain-enabled decentralized role-centric authentication and access management for distributed organizations," Cluster Computing, vol. 24, no. 4, pp. 3551–3571, Jun. 2021.

[4] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar, and S. Ellahham, "Blockchain-based forward supply chain and waste management for covid-19 medical equipment and supplies," Ieee Access, vol. 9, pp. 44 905–44 927, 2021.

[5] H. Baniata and A. Kertesz, "PriFoB: A Privacy-aware Fog-enhanced Blockchain-based system for global accreditation and Credential Verification," Journal of Network and Computer Applications, p. 103440, Jun. 2022.

[6] K. Bhumichitr and S. Channarukul, "Acachain: Academic credential attestation system using blockchain," In Proceedings of the 11th International Conference on Advances in Information Technology, pp. 1-8, 2020.

[7] L. M. Palma, M. A. G. Vigil, F. L. Pereira, and J. E. Martina, "Blockchain and smart contracts for higher education registry in Brazil," International Journal of Network Management, vol. 29, no. 3, p. e2061, Jan. 2019.

[8] A. Tariq, H. B. Haq, and S. T. Ali, "Cerberus: A blockchain-based accreditation and degree verification system,", arXiv preprint arXiv:1912.06812, 2019.

[9] "Boards of Intermediate and Secondary Education | Punjab Portal," www.punjab.gov.pk. https://www.punjab.gov.pk/boards_punjab (accessed Jul. 04, 2022).

[10] IBCC, "Requirements for Attestation," Inter Board Committee of Chairmen. https://ibcc.edu.pk/requirements-for-attestation/ (accessed Jul. 04, 2022).

[11] "Recognised Universities," www.hec.gov.pk. https://www.hec.gov.pk/english/universities/pages/recognised.aspx (accessed Jul. 04, 2022).

[12] "HEC," www.hec.gov.pk. https:// https://www.hec.gov.pk/english/pages/home.aspx (accessed Jul. 04, 2022).

[13] "Ministry of Federal Education and Professional Training," www.mofept.gov.pk. http://www.mofept.gov.pk/ (accessed Jul. 04, 2022).

[14] "What are smart contracts on blockchain? | IBM," www.ibm.com. https://www.ibm.com/ae-en/topics/smart-contracts (accessed Jul. 04, 2022).

[15] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, and M. Omar, "The role of blockchain technology in telehealth and telemedicine," International Journal of Medical Informatics, vol. 148, p. 104399, Apr. 2021.

[16] P. Labs, "IPFS is the Distributed Web". https://ipfs.io/ (accessed Jul. 04, 2022).

[17] A. R. Khan and R. W. Ahmad, "A Blockchain-Based IoT-Enabled E-Waste Tracking and Tracing System for Smart Cities," in *IEEE Access*, vol. 10, pp. 86256-86269, 2022.

[18] A. Rashid and A. R. Khan, "Blockchain-Based Autonomous Authentication and Integrity for Internet of Battlefield Things in C3I System," in *IEEE Access*, vol. 10, pp. 91572-91587, 2022.