Higher Education’s Certificates Model based on Blockchain Technology

Mustafa A. Ali¹ and Wesam S. Bhaya²

¹College of Science, University of Kerbala
²College of Information Technology, University of Babylon

E-mail: Mustafa.a@uokerbala.edu.iq

Abstract. Blockchain technology has revolutionized economic transactions, and it is expected to spread and influence other fields. It can create innovative and destructive effects on the systems that need to be executed, store, verified, and continually update digital data among participating parties. Moreover, it provides security, privacy, trust, and transparency. In the education field, there is a shy presence of some blockchain applications, and the majority of them have a pilot character. Hence, a model based on blockchain is introduced in this study, which aims to provide easy to apply for certificates, as well as share and verify these certificates with a third party. Moreover, the mechanism of the proposed model proposes permanent distributed hashes records of students’ certificates in Higher Education to reduce forgery. In conclusion, the study discussed the opportunities, benefits, features, and challenges are represented by deploying this model in the Higher Education field.

Keywords. Blockchain Applications, Consensus, Automated Certificate Educational Systems, University Digital Certificate.

1. Introduction

In our increasingly interconnected world and with the constantly increasing and evolving use of computer systems in various areas of contemporary life. In addition to the rapid increase in the speed of internet connections and with the fact that most computer users are novice or untrusted, who have sophisticated computers with high-speed internet connection [1]. Consequently, all that lead to facilitate and increase of security threats and abuse rises that facing the digital systems. Therefore, it is necessary to replace or develop other technologies to preserve digital systems from many security threats and adds layers of protection and trust. A powerful opportunity can emerge from utilizing new blockchain technology. This technology is expected to develop various industries objectives such as economic, society, medical, businesses, and education. As a result, it is necessary to explore and identify the advantage and challenges of blockchain technology [2]. Blockchain technology can be defined as a time-stamped and tamper-resistant distributed digital ledger. It can allow validate and secure the transactions and update records in a transparent, synchronized, and decentralized with the consensus of a majority scheme and is considered a part of the fourth industrial revolution.
This mechanism for generating and managing digital data can be effective across sectors, for instance, when it moves toward increasing productivity and automating processes, reducing cost, or promote new organizational and business models [4].

Blockchain technology has numerous advantages, it enables known and unknown parties who do not have a specific trust in each other to exchange any kind of digital assets such as educational and medical records, services, money, goods, or contracts on a peer-to-peer network without the need to central authority to provide the trust [5]. On the other hand, blockchain faces many underlying technical challenges such as bottlenecks, scalability and performance, interoperability, high-energy consumption, and protection of personal and sensitive data, which are, depending on the type of blockchain [5]. Moreover, regulatory and standardization uncertainties about the formal status of this technology also lead to more risks and ambiguity for companies and other organizations that are interested in deploying blockchain or experimenting with it [6].

At present, many of the potential advantages of blockchain are unrealized or yet to be fully examined. Blockchain evolution faces critical questions about the potential effect, added value, or the specific direction of adoption [7]. However, blockchain technology has seen a burst of interest in recent years and it is expected that it will lead to a revolution that will significantly disrupt the way that the data are shared and create prominence in the evolution of the digital world. It is a highly promising field that requires further researches, experiments, and implementation in different areas [8].

This study objectives not only to explore blockchain technology and its features but also to provide a view on the opportunities and challenges for its used within the Higher Education context. So, we designed a model that utilized blockchain features that could be applicable used to secure, fast, online, and accurately generate and verify academic certificates with a few manual work and without the chance to certificates forgery.

After this introduction, the study reviews in section 2, the most related works that discuss the document forgery problem. Section 3 presents the proposed model. In section 4, the outputs of the proposed model based on a set of theoretical points are discussed and lastly the conclusion.

2. Background

The origin of prevalent academic fraud can be traced back to people without educational qualifications who want to become rich, powerful, honor, or being employed in a short period. Unemployed youth, graduates, and potential college students soon learned that intellectual effort and the need for serious study is not required to achieve their wish, instead, seek connections and then obtain forgery credentials by any means [9]. However, hired fraudulent means became broad.

In [10], the researcher explains that academic fraud consists of a broad range of suspicious activities in the academic field, among them is mutating of the content of the certificates, which originated from a legitimate issuer to suit the holder's need. Researchers in [11] defined academic fraud as the intended misrepresentation of academic achievement that may have a harmful consequence on other parties. Another definition of fake degrees has been introduced by [12,13] which describes it as a certificate obtained from a bogus institution (diploma mills) that holds an
original establishment but has not been issued by the claimed institution. Furthermore, another type of academic fraud is both the origin and content of the certificate are fake; however, it may be difficult to disclose them [13]. According to [14], there are various sources of fake degrees including unaccredited degree-granting institutions, degree mills, and corrupt officials at academic foundations.

Document verification is the process taken to ensure that the documents received from the owner are genuine and that the owner is legitimate [15, 16]. The verification of the certificate removes suspicion about the certificate content and the issuer educational institution. Whether the certificate issued by the alleged institution, as well as, the issuing institution is authentic [15, 17]. This always validates the issuing institution and the qualifications provided. The goal of verification is also to ensure that the certificate has not been altered by the holder and whether it has been truly issued to the owner [11, 16-17]. Certificate verification is steps to seeks and trace to ensuring that the certificate is authentic from its source, means of issuance, and other details about the basis for issuance. It is the process that establishes the originality of something using a confirmed technique [18].

Electronic verification was used, to facilitate and automation of some processes, as well as, the authentication can be accomplished instantly, which saves time for all parties. Furthermore, certificates are shared more easily and securely [18, 19]. It is automation and uses some of the appropriate tools such as verification through a web portal without making a central database to ensure data privacy. This technique operates within a digital certificate and facilitates automatic verification of a degree by a third party without the need of the issuing institution [18,19].

An online certificate system is a web-based system that contains a secure database that can be viewed by three levels of users - the issuing institution, the degree holder, and the third party. The institution issues a digital certificate to a graduate student after fulfilling the academic requirements. On the other hand, the student applied the affirmation to access and share the electronic certificate. Meanwhile, a third party (verifier) also inquires into the system webpage to verify the certificate.

Blockchain technology is a distributed digital ledger with the consensus of a majority scheme that promotes systems that need to be executed, store, verified, and continually update digital data among participating parties. Distributed ledger technology protects and retains the transaction recording and asset tracking and sharing in a decentralized manner [20].

Through the previous studies, it can be noted the there are big problems with forging official documents and the methods to verify these documents. This research aims to propose a model based on permission blockchain that stores compact data proofs of academic certificates in a decentralized database that enables students easy to apply certificates and easy methods to verify and share with a third party.

3- The Proposed Model

In this section, we will describe and illustrate the phases and workings steps of the proposed model. We start with a high-level overview of the main phases in the proposed model. The research aims to
design a model for a trust system to exporting, securing, and ensure the validity of the higher certifications of graduate students.

The main advantage of the proposed model is to ensure the validity of students' certificates in a safe, direct, trust, and fast manner. It also allows students to electronically request a copy of the certification. The proposed model store the validity of academic certificates in a safely electronically compact method depending on blockchain technology. Furthermore, it allows ensuring the validity of students' academic certificates by any interested verifier and from anywhere. This model proposed a permission blockchain distributed system to deployed verifications of students' certificates to prevent the process of forgery certificates, as well as to add transparency and trust in the issuing and export process by ensuring the authenticity of the issuance of those documents. The permission blockchain proposed by the model involved in all student affairs departments belongs to universities of the Ministry of Higher Education. It allows the network participating to add, update, and confirm the student's certifications by a consensus mechanism.

The hash function was used to obtain a one-way encrypted and compressed copy of the students' certifications, and these hashes are stored on the blockchain after the verification processes by participants parties are done. As a result of using the proposed techniques above in the proposed model, we prevent the process of issuing a tampered certificate. Furthermore allowing non-participants parties of blockchain networks such as other companies and organizations to securely and instantaneously check the validity of the student's certificate that is provided to it.

The proposed system includes three main stages, which are issuing certificates, demanding the creation of certification, and verifying the validity of the certifications. Each one of these phases
will be explained in the following sections. Fig. 1. Show workflow of research proposed model.

Fig. 1. Proposed Model Work Flow

3.1 Students Certificates Issuer

The first phase of the proposed model work begins with the process of submitting the graduating student's grades by the department's examination committee to the proposed central system of the university. After completing this process, the system directs these results to the dean of the faculty, the person who in charge, or the person with authority and here there are two cases. The first case is returning the results to the examination committee for modification within the terms and conditions. The second case agrees to approval (consider as a signed) and issue students' grades and certificates. Then the each signed students’ certificate is hashed by the system and forwarded with the hashes to the college’s registration department. As well as the same copy of these certificates is sent to the student affairs department at the university. The output of the hash function is a string of a certain length, which is the hash value. The proposed model extracting the hash value for each student's certificate separately which is considered a verification checksum for each certificate.

After receiving certificates carried out by the approval of the authority holder, these certificates with their hashes are stored in a local database individually by the college’s registration department and the student affairs department at the university. The system sent and deploy only hash values on the universities' blockchain network if the match of hash values occurs between the Student Affairs Department compared with the College Register Department for the same certificates, and if no match means suspicious altering has occurred in certificates, and a person with authority revisions are required. Fig.2. show the steps of certifications issuer.

![Fig.2. Steps of Certificates Issuer](image)

3.2 Request the Student’s Certificate
The proposed system allows any graduated students from any one of the participating universities in this system to request a graduation certificate from anywhere in the world at any time. It provides a portal or application based on the Internet that allows the student to request an addressed certificate to the desired destination according to the rules. In the case of using the portal, the student should enter important information such as the full name, college, department, and the destination to which the certificate is to be addressed in addition to a valid email address. The certificate issued is sending to the student's email address. In the case of using the application, it will be an electronic wallet in which the student receives and save all the certificates issued to him. Furthermore, by this wallet, all the details of the student can be identified through a specific serial number or a public key when contacting the system or when requesting the certificate. It also saves all previously issued certificates.

Upon receiving the application submitted by the student to get the academic certificate, the system will verify the student’s identity and whether he has the right to apply for the certificate. If the information provided by the student is correct, the system will direct the application to the registration department in the specified college for the required procedure. The Registration Department performs a first validity check by extracts the student's information and grades stored locally and calculates the hash value for this information and compares it with the hash value stored on the blockchain network to ensure that there is no tampering with locally stored certificate information. Upon completion of the verification of the validation process of the students' information, this information with the destination to which the certificate is to be addressed that taken as requested from the student shall be submitted as an unsigned student certificate issued to the Dean’s office for approval (signing).

After obtaining the approval of the dean, the date and number of the certificate issued are given by the system. To deploy the newly created certificate information, it is sent to the Student Affairs Department that performs a second validity check by calculating the hash value of the new certificate's main information and comparing it with the stored hash value in the universities blockchain network. When a match occurs, it means that there is no tampering with the newly created certificate main information and sends a newly created hash value of the new student certificate to the blockchain network to be approved and stored.

After obtaining the approval of the members participating in the network to publish and store the value of the new hash, the process of storing the new hash is performed and a confirmation message sends to the system. Upon completion of the storage process, a copy of the certificate required by the system is sent to the student's electronic wallet or via the electronic email, as mentioned previously. Students can also go to the college’s registration department to receive the hard copy of that attested certificate.
3.3 Validations of Certificates

This phase is considered the practical and actual result of the system, as it represents the benefit of applying the proposed model. Actual works of this phase begin when an institution or a company wanted to verify the validity of the certificates submitted to it to obtain the advertised position. As the proposed system provides a webpage or application that can be accessed from anyone, any time, and anywhere in the world without the need to participate or pay for the system. The gate could be a portal or an application based on the Internet, which enables anyone to verify the correctness of the students’ certification instantly. Even when the absence of the institution that granting this certificate for any reason, such as stopping its work or being exposed to any natural or intentional disaster such as fires or floods.

When the graduate student provides his gained higher certificate information to obtain a specific position within a specific company (get hire). Therefore, the company or organization needs to verify the validity of the submitted certificate from the concerned person. In this case, the company employer can verify the validity of the provided certificate in a real, reliable, and safe way through a portal belong to the system.

The work of this phase begins when enters only the important information of the certificate which is the name, average grade, date, issue number, agency, or the certificate is uploaded electronically (if the certificate is submitted to the company electronically) through the portal by an employer in the company. The received information of the certificate submit to the portal is entered at the same hash function used when creating and stored the original certificate hash on the blockchain network. Then a query is created to perform a search for a match of the generated hash within universities blockchain network stored hashes. If a match is found means that the certificate information is correct and the validity message will be shown.

If there is no match for any reason such as a mistake in the entry process or a process that changes any information from the certificate information (forging the certificate). In this case, there will be no match of the stored hashes on the blockchain network and the system will be shown a message of failure or error through the portal. Fig.4. show steps to verify the certificate.
4. Results and Discussion

To understand the expected outputs from applying this model to the certificates system, it must be compared with the current systems of the issuer the paper and electronic certificates. Moreover, explain the problems and weaknesses to solve or enhance them using blockchain technology. This section describes the most important problems in the current systems.

Certifications acquired over a long period from different accredited educational institutions throughout the country or the world, need to be approved for their originality. The verified process is becoming more difficult and takes long periods due to the increase in the number of universities, colleges, courses, and students. Educational institutions spend a lot of time, effort, and resources in creating academic certificates for students as well as verifying transcripts and data starting from their date’s births, records of accomplishment, and capabilities.

The trust, security, transparency, and speed along with automation through digitization are offered by blockchain technology that comes as leverage to the education industry across the world. The results of adopting the proposed model are summarized below:

1- Easy Verification Mechanism and Accurate Information: A portal can be used by the third-party who want to verify the certificate.

2- Convenient: The students need to no longer provide many papers with proof of their originality each time they use to apply for a job.

3- Cost-effective: The digitization of the process of the creation and validation of the certificates reduces the costs for all parties.

4- Time-efficient: The increased speed of creating and verifying the certificates as the certificates can be delivered and verified digitally.

5- Data Privacy and Security: Students' academic achievement is stored in the local and private database of an educational institution, as well as store hashes of those credentials, which are stored on the blockchain that is cryptographically protected. As result, prevent the issuance of forgery certificates and at the same time, students' creational is safe and reliable.

6-. Secure Transactions, Transparent, and Immutable Data: The hashes are approved and authorized by a consensus mechanism. Moreover, all blockchain participants store the same transactional data that vastly improve the trust in the whole system.

7- Availability: The verification of certificate is there at any time and from anywhere even when the problem of unavailability of the educational institution such stops using the network, that their equipment malfunctions, or even stop institution work.

On the other hand, to develop a reliable and secure blockchain certificate system with high functionality and usability, a group of solid technical and mathematical foundation experts of blockchain is needed. This presents a shortcoming for practitioners and researchers in the field of
education. Blockchain technology is difficult to comprehend by educators, learners, and other professional parties. Universities need to know how the adoption of the blockchain will affect their privacy, database rights, and other confidential information. This study aims to establish a model for blockchain technology accreditation for certificate verification systems but does not address the technical aspects of implementation. Further studies will be necessary to realize the implications of adopting this technology for enhanced implementation.

5. CONCLUSION

The development of distributed and secure electronic systems has become an important subject in line with the development of the digital world. The application of blockchain technology is an excellent example of these systems that provides exciting features such as transparency, trust, and decentralization with untampered and permanent data records. The implementation of such technology to systems for issuing students' certificates, especially when the individuals are subject to many academic studies and training from several different institutions and they obtain several certificates, is critical. The process of preserving these certificates in a way that is permanent, not tampered with, or forged is very important. Moreover, it is important to present an opportunity for third parties to verify shared certificates quickly, securely, and independently. The proposed model fulfills for preventing forgery certificates and managing digital academic credentials mainly in terms of the trust, high outputs, availability, transparency, low costs, and resource consumption, especially with the existence of many educational institutions nowadays. This study does not address the technicalities of implementation. Further studies to design and facilitate the creation and implementation of the blockchain solution in education are recommended.

References

[1] Bhaya, W. S., & Ali, M. A. (2017). Review on Malware and Malware Detection Using Data Mining Techniques. Journal of University of Babylon for Pure and Applied Sciences, 25(5), 1585-1601.

[2] Schwab, K. (2017). The fourth industrial revolution. Currency.

[3] Bozic, N., Pujolle, G., & Secci, S. (2016, December). A tutorial on blockchain and applications to secure network control-planes. In 2016 3rd Smart Cloud Networks & Systems (SCNS) (pp. 1-8). IEEE.

[4] Chang, S. E., Chen, Y. C., & Lu, M. F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. Technological Forecasting and Social Change, 144, 1-11.

[5] Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of Blockchain technology: pros, cons and SWOT. Cluster Computing, 22(6), 14743-14757.

[6] De Filippi, P. D. F. (2018). Blockchain and the law: The rule of code. Harvard University Press.

[7] Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. International Journal of Information Management, 49, 114-129.
[8] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), e0163477.

[9] Murray, D. E. (1993). Letters of credit and forged and altered documents: some deterrent suggestions. Com. LJ, 98, 504.

[10] Effiong, M. E. A FRAMEWORK FOR THE ADOPTION OF BLOCKCHAIN TECHNOLOGY IN ACADEMIC CERTIFICATE-VERIFICATION SYSTEMS: A CASE STUDY OF NIGERIA.

[11] du Plessis, L., Vermeulen, N., van der Walt, J., & Mackela, L. (2015). Verification of Qualifications in Africa. Research report on the Verification of Qualifications in Africa, Northwest University, South Africa supported by the South African Qualifications Authority.

[12] Haciroyakipoglu, G., Hui, J. Y., Suguna, V. S., Leong, D., & Rahman, M. F. B. A. (2018). Countering fake news: A survey of recent global initiatives.

[13] Johnson, D. A. (2020). ‘An Underworld in Education’: The Demise of Missouri’s Medical Diploma Mills. Social History of Medicine, 33(1), 106-131.

[14] Garwe, E. C. (2015). Qualification, award and recognition fraud in higher education in Zimbabwe. Journal of studies in education, 5(2), 119-135.

[15] Houser, P. B., & Adler, J. M. (1997). U.S. Patent No. 5,606,609. Washington, DC: U.S. Patent and Trademark Office.

[16] Balsubramanian, S., Prashanth, I. R., & Ravishankar, S. (2009, August). Mark sheet verification. In 2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication (pp. 359-362). IEEE.

[17] Beattie, D. D., Creighton Jr, N. L., Bailey, C. T., Remy, D. L., & Hamandi, H. (2006). U.S. Patent No. 7,003,661. Washington, DC: U.S. Patent and Trademark Office.

[18] Badr, A., Rafferty, L., Mahmoud, Q. H., Elgazzar, K., & Hung, P. C. (2019, June). A permissioned blockchain-based system for verification of academic records. In 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-5). IEEE.

[19] Saleh, O. S., Ghazali, O., & Rana, M. E. (2020). Blockchain based framework for educational certificates verification. Journal of critical reviews, 7(3), 79-84.

[20] Laurence, T. (2019). Blockchain for dummies. John Wiley & Sons.