Driving Digital Transformation in Certificate Management: A Blockchain-Based Solution for Vinh University

Le Van Tan[1] and Pham Minh Hung[2,*]

[1]Cyber School, Vinh University, Vinh, Nghe An, Vietnam
[2]College of Education, Vinh University, Vinh, Nghe An, Vietnam
Email: tandhv@vinhuni.edu.vn (L.V.T.); hungpm@vinhuni.edu.vn (P.M.H.)
[*]Corresponding author
Manuscript received August 17, 2023; revised September 26, 2023; accepted October 23, 2023; published January 25, 2024

***Abstract*—In today's digital age, secure and reliable certificate management is crucial for validating achievements and establishing credibility. Traditional methods face challenges such as fraud and cumbersome verification processes. However, blockchain, digital signatures, and QR codes offer a more secure and streamlined approach. Vinh University, renowned for its teacher training and educational research, annually grants thousands of diplomas and certificates. This paper presents a customized Certificate Management System for Vinh University, which utilizes blockchain, digital signatures, and QR codes to ensure integrity and simplify verification. By integrating these technologies, this system not only upholds the integrity of certificates but also sets a new standard for efficient and trustworthy verification processes in the digital age. Implementing this certificate management system represents a significant advancement in certificate management, promising to enhance the credibility and reputation of Vinh University while benefiting its graduates and other stakeholders.**

***Keywords*—blockchain, certificate management, digital transformation, QR code**

I. Introduction

Nowadays, the importance of secure and reliable document management systems cannot be overstated. One particular area that demands an efficient and tamper-proof solution is the management of certificates. From educational degrees to professional certifications, certificates play a vital role in validating achievements and establishing credibility.

Traditional methods of certificate management often face challenges such as the risk of fraud, counterfeiting, and cumbersome verification processes. However, the emergence of blockchain technology, digital signatures, and QR codes has paved the way for a more secure and streamlined approach to certificate management [1–5].

Vinh University, recognized as a prominent university for teacher training, educational research, and technology transfer, is dedicated to the success of its students. Each year, the university grants diplomas and certificates to thousands of graduates, encompassing students, trainees, and doctoral candidates. Consequently, the demand for verifying these certificates from various agencies, organizations, and individuals is significant. In 2020, Vinh University responded to more than 1,000 requests for diploma and certificate verification from external entities, requiring the retrieval of original documents and a thorough review before issuing a written response. The traditional certificate verification process usually takes 3–5 working days and involves several key steps: receiving documents, verifying them, and providing a response. Vinh University issues over 3,000 certificates annually, which makes the comparison with original documents time-consuming, especially for significantly older certificates. Keeping records on paper poses a risk of damage over time. Inspection officers focus solely on reviewing the information relevant to stakeholders' needs and comparing it with stored data for verification. This manual process, involving multiple departments and varying timelines depending on the data's age and mode of communication, poses challenges regarding efficiency and resource allocation.

This paper presents an overview of designing a Certificate Management System that harnesses the power of blockchain, digital signatures, and QR codes specifically tailored for Vinh University. By leveraging these technologies, organizations can ensure the integrity, authenticity, and accessibility of their certificates while simplifying the verification process for all stakeholders.

The rest of this paper is structured as follows. Section II focuses on the literature review and presents an overview of techniques used in this study, including blockchain, digital signature, and QR code. Section III delves into the research methodology, encompassing research questions and the search strategy employed. Section IV presents the research question results. The final section concludes the paper and identifies important further work.

II. Literature Review

Various researchers have explored the potential applications of blockchain technology in the field of education. Chen *et al*. [6] introduced the features and advantages of blockchain technology and discussed its potential applications in education. They proposed innovative applications and highlighted the benefits and challenges of using blockchain in education. Yumna *et al*. [4] focused on the issues faced by educational institutions in three areas: physical, digital, and financial. They analyzed the risks of manipulation, difficulties in verification, and exchanging records between institutions. Kamisalic *et al*. [2] presented use cases of blockchain in education, including streamlining diploma verification, creating virtual lifetime learning passports, securing certificates permanently, verifying accreditation processes, and automating credit recognition. Alammary *et al*. [1] focused on three main themes: developed educational applications using blockchain, the potential benefits of blockchain in education, and challenges in adopting blockchain technology. The researchers examined existing projects and protocols that utilized blockchain in the

educational domain. Fedorova and Skobleva [7] published a paper titled "*Application of Blockchain Technology in Higher Education*". The paper analyzed the opportunities and restrictions associated with the application of blockchain in higher education. Recently, an increasing number of researchers have focused on exploring the potential research and applications of digital transformation [8–11] and blockchain in the field of education [12–21]. Blockchain technology has numerous applications in the field of education, such as certificate management, competencies and learning outcomes management, evaluating students' professional ability, copyrights management, examination review, and supporting lifelong learning, among others [1, 2].

A. Blockchain in Education

Blockchain in education refers to applying blockchain technology within the educational sector. Blockchain is a decentralized digital ledger that records transactions or data across multiple computers or nodes. In education, blockchain offers a transparent, secure, and tamper-resistant platform for storing, verifying, and sharing educational records, credentials, and other relevant data [1, 16].

By utilizing blockchain, educational institutions can improve the integrity and efficiency of administrative processes, such as record-keeping, credential verification, and student enrollment. It enables the creation of a decentralized and trustless environment where academic achievements, certifications, and other educational data can be securely stored and accessed by relevant stakeholders, including students, employers, and educational institutions.

The decentralized nature of blockchain ensures that data stored on the network is resistant to alteration or tampering, enhancing the credibility and reliability of educational records. Additionally, blockchain's transparency and immutability can facilitate greater trust among parties, simplify administrative procedures, and streamline processes like credit transfer, accreditation, and lifelong learning [16].

B. Digital Signatures in Education

Digital signatures play a crucial role in ensuring the integrity, authenticity, and non-repudiation of electronic documents and transactions within the education sector. A digital signature is a cryptographic mechanism that enables individuals or institutions to sign digital documents, similar to how a handwritten signature is used to sign physical documents [5].

In education, digital signatures provide a secure and efficient method for verifying the authenticity of educational records, such as transcripts, certificates, and diplomas. By digitally signing these documents, educational institutions can ensure they have not been tampered with and originate from a trusted source.

Digital signatures also facilitate the secure exchange of documents between educational institutions, students, and employers. They enable the verification of the document's integrity and the identity of the signatory, eliminating the need for physical paperwork and allowing for faster and more reliable document processing [22].

C. QR Codes in Certificate Verification

QR (Quick Response) codes are widely used in certificate verification processes to provide a quick and efficient method of verifying the authenticity and validity of certificates. QR codes are two-dimensional barcodes that can store much information, such as a unique identifier or a link to an online verification platform.

In certificate verification, QR codes are often printed on physical certificates or included in digital certificates. Scanning the QR code using a smartphone or a QR code reader directs the verifier to a specific website or application containing the necessary verification information.

The verification platform associated with the QR code typically provides details such as the certificate holder's name, the issuing institution, the date of issuance, and any relevant additional information. By accessing this information through the QR code, verifiers can quickly validate the certificate's authenticity and confirm its legitimacy [3].

III. Methodology

A. The Certificate Verification Process

In this section, we present a certification verification process applied to Vinh University, which is depicted in Fig. 1. The process in this figure involves a series of closely related actions to ensure the authenticity and validity of a certificate issued by the university.

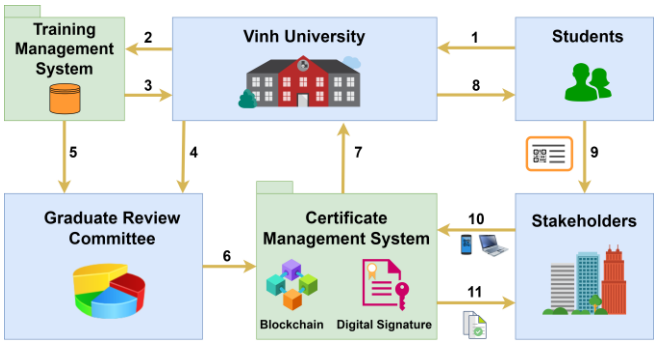

Fig. 1. The certificate verification process applied to Vinh University.

By following these steps, stakeholders can effectively verify the authenticity and validity of certificates, ensuring the credibility and reliability of Vinh University's educational credentials. The steps are detailed as follows:

Step 1: Students Enroll at University

The journey begins with aspiring students enrolling at Vinh University, where they embark on their educational pursuits. Through a well-established admission system, students provide their personal and academic information, which is the foundation for their academic journey.

Steps 2 and 3: Vinh University Stores and Updates Students' Information

During the study, Vinh University diligently stores and updates students' course information in a training management system. This digital repository ensures the accuracy and accessibility of crucial student data throughout their academic tenure. From personal details to academic performance, all relevant information is securely recorded, creating a reliable and up-to-date digital record.

Step 4: Establishment of Graduation Review Committee

As students approach their graduation, qualified students will undergo a review by the previously established training council. This council will assess the student's fulfillment of academic requirements and ascertain their eligibility for graduation.

Step 5: Graduation Review Data from the Training Management System

To facilitate the graduation review process, the committee accesses the training management system. This system serves as a centralized source of graduation-related data, enabling the committee members to review students' academic performance, course completion, and any other relevant criteria necessary for certification.

Steps 6 and 7: Transfer of Graduation Data to Certificate Management System applying the Blockchain and Digital Signatures Technology

Upon completing the graduation review, Vinh University transfers the graduation data from the training management system to a cutting-edge certificate management system. This system leverages blockchain technology's power to ensure the graduation data's authenticity and immutability.

Blockchain and digital signature technologies are applied to the graduation data in the certificate management system. This integration enables stakeholders to verify the legitimacy of the certificates through a trustless and decentralized system. The blockchain guarantees the integrity and transparency of the data. Data integrity is maintained because altering one block in a decentralized system is exceptionally challenging, guaranteeing the permanence and reliability of certificate-related data. Moreover, transparency is a core feature facilitated by the decentralized ledger, providing all authorized participants with real-time access to identical information. This transparency fosters trust and eliminates the need for centralized authorities, enhancing the credibility of the certificate management system.

Meanwhile, digital signatures serve the purpose of enhancing security, preserving integrity, and validating the authenticity of the training institution. The process involves the following steps:

1) generating an electronic diploma;
2) obtaining the signature of the head of the university;
3) applying the official stamp containing the unique identification number of the training institution.

Regarding the integrity of the signed data, any alteration to the document after it has been signed will invalidate the signature, alerting users to potential tampering. Remarkably, the process of using digital signatures in the certificate management system is carried out through the following stages: (i) obtaining a digital certificate from a trusted authority containing a public key and identity details, then creating a unique digital signature using a private key; (ii) embedding the digital signature in the certificate, either as a separate file or within its structure; (iii) storing the digitally signed certificate securely and sharing it with those needing to verify its authenticity; (iv) using the public key to decrypt the digital signature, confirming the certificate's validity and integrity through a hash comparison.

Step 8: Vinh University Issues Certificates to Students

Empowered by the certificate management system, Vinh University effectively manages the graduation data and expeditiously issues certificates to deserving students. Integrating blockchain technology ensures that the certificates are tamper-proof, tamper-evident, and resistant to fraudulent activities.

Step 9: Students Submit Documents to Employers

Armed with their university knowledge and skills, students submit their necessary documents, such as resumes, certificates, and academic transcripts, to potential employers. This step serves as a crucial bridge between academic achievements and professional opportunities.

Step 10: Verification of Certificates by Employers

To verify the authenticity of candidates' certificates, employers can utilize the front-end system of the certificate management system. They can either scan the QR code on the certificate or manually enter the certificate information into the system. This process grants employers quick and reliable access to the candidates' certification details.

Step 11: Data Verification and Feedback from Certificate Management System

The certificate management system, backed by blockchain technology, verifies the stored data information against the blockchain ledger. Through this verification process, the system ensures the accuracy and integrity of the certificates. Employers receive immediate feedback, giving them confidence in the credibility of the candidate's qualifications.

B. The Certificate Management System

The Certificate Management System of Vinh University is a comprehensive platform that integrates various components to manage certificates effectively. It consists of both back-end and front-end components to ensure the secure and efficient management of certificates. Here is an overview of the system:

Blockchain: The back-end of the Certificate Management System incorporates blockchain technology to provide a decentralized and tamper-resistant ledger for storing and managing certificate-related data. Blockchain ensures the immutability and integrity of certificates, preventing unauthorized modifications.

Digital Signature: The system utilizes digital signature mechanisms to authenticate and verify the validity of certificates. Digital signatures provide cryptographic proof of the certificate's integrity, ensuring that it has not been altered or tampered with.

Web-based System: The front-end component of the Certificate Management System is a user-friendly web-based interface accessible to stakeholders such as educational institutions, students, employers, and verification authorities. This interface enables seamless interaction and access to certificate-related functionalities.

Stakeholder Access: Different stakeholders have specific roles and access levels within the system. The university can issue, manage, and update certificates. Students can view and share their certificates. Employers and verification authorities can authenticate and verify certificates.

Due to limited space, we will focus on presenting a selection of techniques for constructing blockchain database tables including: *Type_of_Certificate*, *Certificate_Decision*, *Certificate*, and *Transaction* tables. To gain a comprehensive

understanding of these tables, their intricate relationships, and the underlying data schema, we encourage readers to refer to Fig. 2 for the Entity-Relationship diagram. A detailed description of the tables is provided as follows:

1) Table Type_of_Certificate

The initial and crucial aspect of certificate management involves classifying various types of certificates. The "Type_of_Certificate" table contains information about a wide range of certificates, including PhDs, Master's degrees, engineering, and bachelor degrees, as well as specialized certifications such as English, physical, and defense education certificates, among others. Each type of certificate represents a unique level of achievement or specialization within a specific field. This classification not only aids in efficient storage and retrieval but also enables customized verification processes based on the specific attributes associated with each certificate type.

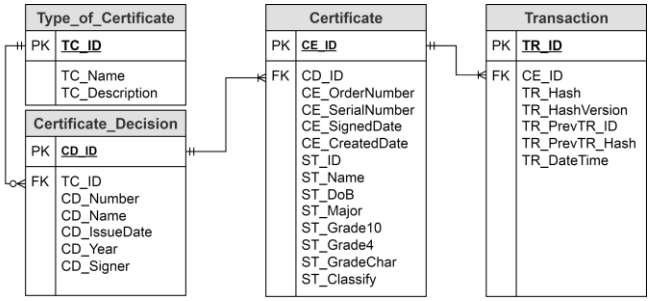

Fig. 2. A part of Entity-relationship diagram for the certificate management system.

2) Table Certificate_Decision

The relationship between table Type_of_Certificate and Certificate_Decision is 1-many. The "Certificate_Decision" table serves as a mechanism for educational institutions to determine the recognition and validity of certificates. The university makes decisions regarding certificate recognition in batches. This process allows for consistent evaluation and assessment of certificates based on established criteria and standards. By associating each certificate with its respective decision batch, institutions can ensure transparency and accountability in the recognition process.

3) Table Certificate

The "Certificate" table contains essential information that not only appears on the physical certificates but also serves as a foundation for generating secure and tamper-proof blockchains. This information might include the recipient's name, academic institution, degree or certification title, date of completion, and any relevant additional details. Including this data in the blockchain allows for easy verification and authentication of certificates, eliminating the need for cumbersome manual processes.

4) Table Transaction

The Transaction table stores information related to the blockchain to facilitate the seamless integration of certificates with blockchain technology. The attributes within this table, such as TR_Hash, TR_HashVersion, TR_PreTR_ID, and TR_PreTR_Hash, are used to track and record transactions on the blockchain. These fields ensure the transparency and immutability of the certificate-related data, making it resistant to unauthorized alterations or falsification. A detailed description of fields in this table is as follows:

TR_Hash: The SHA256 hash generated by combining all related fields in the Certificate table. Particularly, TR_Hash = SHA256 (CE_OrderNumber + CE_SignedDate + CE_SerialNumber + CE_CreatedDate + ST_ID + ST_Name + ST_DoB + ST_Major + ST_Grade10 + ST_Grade4 + ST_GradeChar + ST_Classify).

TR_HashVersion: This field allows adding fields to the table or addressing bugs in the hash logic without compromising compatibility with older entries.

TR_PreTR_ID: Refers to the preceding TR_ID in sequence with a unique index on this field; only one NULL value (the genesis block) and one child per parent is permitted.

TR_PreTR_Hash: The TR_Hash of the row referenced by TR_PreTR_ID. This value is included in the hash of the current row, encapsulating all preceding data within a single hash. Any alteration made to past data would require recomputing all hashes from that particular row onward.

The TR_PreTR_Hash provided here is derived from the row associated with TR_PreTR_ID. This hash is incorporated into the hash of the current row. As a result, all previous data is condensed into this one hash. If any modifications were made to past information, it would require recalculating all hashes from that specific row onwards.

IV. Results

A blockchain system has been implemented including three nodes (server) at the IT Center, Quality Assurance Center, and Training Department in Vinh University. By leveraging blockchain technology, these nodes are seamlessly interconnected, forming a robust network that revolutionizes data handling and ensures the integrity of information.

As a central hub, The IT Center plays a pivotal role in implementing and maintaining the blockchain system. It oversees the technical aspects, including blockchain infrastructure setup, configuration, and ongoing management. This node serves as the backbone of the entire system, ensuring its stability and security.

The Quality Assurance Center acts as a critical node responsible for verifying and validating data within the blockchain network. Its role is to ensure the accuracy and authenticity of information, guaranteeing that only valid and reliable data is added to the blockchain. Through rigorous quality checks and audits, the Quality Assurance Center upholds the integrity of the system.

The Training Department's blockchain node is entrusted with the crucial responsibility of adding new certificate records to the system. When a new certificate is issued, the Training Department's node meticulously inserts the relevant information into the blockchain, creating an immutable record. This process guarantees the authenticity and integrity of the certificates, eliminating the risk of fraudulent activities or unauthorized modifications. By leveraging blockchain technology, the Training Department can maintain a transparent and trustworthy certification system, instilling confidence in the validity and reliability of the certificates issued.

The collaboration between the IT Center, Quality Assurance Center, and Training Department establishes a foundation for secure and reliable data handling, ensuring the

organization remains at the forefront of technological advancements in blockchain.

Following an extensive research and experimental development phase, Vinh University has successfully deployed its diploma and certificate management system, which is now available at https://diploma.vinhuni.edu.vn (see Fig. 3). Users can access the system and utilize its support services through the following methods:

Method 1: Scan the QR Code using a Smartphone

Utilize the camera or QR code scanning feature on a smartphone. The certificate information page will be instantly displayed on the phone screen.

Method 2: Access to the following website on a web browser: https://diploma.vinhuni.edu.vn

Visit the mentioned web address and enter the following information: *Lookup code*, *Full name*, *Date of birth*, *Year of graduation*, or *Serial number*. The system will search based on the provided information and present the corresponding search results.

Method 3: Directly access the address in a browser using the syntax: https://diploma.vinhuni.edu.vn#[Lookup code]

The lookup code, printed on each student's certificate, is designed to ensure information security by encoding it into a string of characters. This encoding makes it challenging for other system users to guess the code. By employing this approach, the system safeguards the privacy and integrity of the certificate information, allowing only authorized individuals to access and retrieve the relevant data.

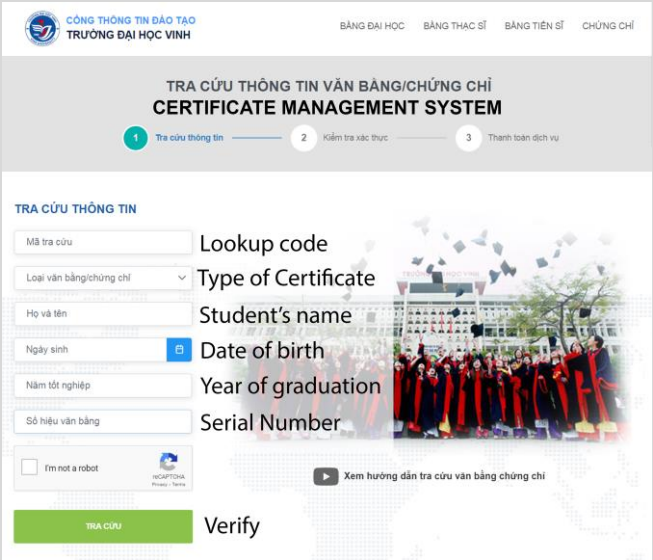

Fig. 3. Vinh University certificate management system user interface.

By employing these convenient methods, users can easily access and utilize the Vinh University diploma and certificate management system, providing a streamlined experience for verifying and retrieving certificate information.

V. Discussion

Since its successful implementation in 2021, introducing this system has proven immensely advantageous for the university. One of the most notable benefits lies in the significant simplification and efficiency improvement in the certificate verification process. Previously, the verification of certificates required labor-intensive manual procedures, resulting in substantial costs and time investment. However, with the advent of this system, the entire certificate verification process has been seamlessly transitioned to an online platform, eliminating the need for cumbersome offline verification methods.

In the pre-system era, the university was burdened with verifying more than a thousand certificates annually, which was arduous and time-consuming. However, with the integration of this advanced system, the verification process has been revolutionized. Users can now verify their certificates by following the simple steps outlined above, thus preventing the need for tedious manual verification procedures. This streamlined approach has significantly reduced the labor and costs associated with the certificate verification process, allowing the university to allocate resources more efficiently toward other vital aspects of education and administration.

Furthermore, the transition to online certificate verification has also enhanced the overall user experience. By leveraging the system's user-friendly interface, individuals can effortlessly access and verify their certificates, eliminating the hassle of physical document submission or in-person visits. This accessibility and convenience have empowered students, alumni, and other stakeholders to swiftly and securely validate their credentials, providing them with a sense of reassurance and confidence in the integrity of their certificates.

Moreover, implementing this system has paved the way for improved data security and confidentiality. By adopting stringent encryption techniques and incorporating robust information security measures, the system ensures that sensitive certificate information remains protected from unauthorized access. The encoded lookup codes assigned to each certificate serve as an additional layer of security, making it exceedingly difficult for unauthorized individuals to decipher or manipulate the data. This heightened security framework not only safeguards the privacy of individuals' personal information but also fortifies the credibility and authenticity of the university's certificate verification process.

VI. Conclusion

Implementing a secure and reliable Certificate Management System utilizing blockchain technology, digital signatures, and QR codes has revolutionized the certificate management and verification process at Vinh University. The system has brought numerous benefits, including a streamlined and efficient verification process, reduced labor and costs, enhanced user experience, and improved data security. By embracing these technological advancements, Vinh University has positioned itself at the forefront of certificate management, ensuring the integrity and authenticity of its certificates while providing a seamless and trustworthy experience for all stakeholders involved.

While implementing a Certificate Management System utilizing blockchain technology brings numerous benefits, it is essential to acknowledge certain drawbacks of this innovative approach. One such drawback is the potential impact on search speed when retrieving information from the system. Unlike traditional systems that rely on centralized

databases, blockchain-based systems require authentication on different nodes to ensure data integrity and prevent tampering.

When a user performs a search, the system must authenticate the information across multiple nodes in the blockchain network. Although essential for maintaining the system's security and trustworthiness, this decentralized verification process can result in slightly slower search times than centralized systems. Each node in the network must independently validate and confirm the requested information, which introduces additional steps and communication overhead.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Pham Minh Hung is responsible for the introduction and literature review sections, along with proposing ideas for the methodology section, while Le Van Tan handles all the remaining content in this paper. All authors had approved the final version.

REFERENCES

[1] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain—based applications in education: A systematic review," *Applied Sciences*, vol. 9, 2019. [1]

[2] A. Kamisalic, M. Turkanovic, S. Mrdovic, and M. Hericko, "A preliminary review of blockchain-based solutions in higher education," in *Proc. International Workshop on Learning Technology for Education in Cloud*, *Communications in Computer and Information Science*, vol. 1011, pp. 114–124, 2019.

[3] A. Tariq, H. Binte Haq and S. T. Ali, "Cerberus: A blockchain-based accreditation and degree verification system," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 4, pp. 1503–1514, 2023. [3]

[4] H. Yumna, M. M. Khan, M. Ikram, and S. Ilyas, "Use of blockchain in education: A systematic literature review," in *Proc. Asian Conference on Intelligent Information and Database Systems*, LNAI, 11432, pp. 191–202. 2019.

[5] J. Katz, "Digital signatures: Background and definitions," *Digital Signatures*, Springer, 2010.

[6] G. Chen, B. Xu, M. Lu, and N. S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learning Environments*, vol. 5, 2018.

[7] 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, 2020.

[8] B. R. Aditya and Andrisyah, "Digital transformation in early childhood education: Teachers' self-regulated model for digital learning," *International Journal of Information and Education Technology*, vol. 13, no. 2, pp. 329–334, 2023.

[9] B. R Aditya, R. Ferdiana, and S. S. Kusumawardani, "Categories for barriers to digital transformation in higher education: An analysis based on literature," *International Journal of Information and Education Technology*, vol. 11, no. 12, pp. 658–664, 2021.

[10] R. Latifah, C. W. Budiyanto, and H. Saputro, "Digital transformation readiness in education: A review," *International Journal of Information and Education Technology*, vol. 12, no. 8, pp. 809–815, 2022.

[11] T. S. Hoang, N. T. M. Loc, P. N. Long, N. T. T. Huyen, and N.T. Loan, "Digital competence of lecturers at the universities of education: In the context of education digital transformation Vietnam," *International Journal of Information and Education Technology*, vol. 12, no. 10, pp. 1085–1089, 2022.

[12] B. Hameed, M. M. Khan, A. Noman, M. J. Ahmad, M. R. Talib, F. Ashfaq, H. Usman, and M. Yousaf, "A review of blockchain based educational projects," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 10, pp. 491–499, 2019.

[13] B. S. Nur, P. Rehana, H. Farjana, A. N. Murad, Z. A. Zaman, and M. F. Mridha, "Blockchain based architecture for certificate authentication," in *Proc. the International Conference on Innovative Computing & Communication* (ICICC), pp. 1–10, 2021.

[14] C. Alex and F. Inguanez, "BlockChain based certificate verification platform," *Business Information Systems Workshops*, *Lecture Notes in Business Information Processing*, vol. 339, pp. 211–216, 2019.

[15] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learning Environments*, vol. 5, no. 1, pp. 1–10, 2018.

[16] G. Alex and A. F. Camilleri, "Blockchain in education," *Joint Research Centre*, 2017.

[17] H. Bushra, M. M. Khan, A. Noman, M. J. Ahmad, M. R. Talib, F. Ashfaq, H. Usman, and M. Yousaf, "A review of blockchain based educational projects," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 10, pp. 491–499, 2019.

[18] J. Guo, C. Li, G. Zhang, Y. Sun, and R. Bie, "Blockchain-enabled digital rights management for multimedia resources of online education," *Multimed Tools Appl*. vol. 79, pp. 9735–9755, 2020.

[19] J. Kaneriya and H. Patel, "A secure and privacy-preserving student credential verification system using blockchain technology," *International Journal of Information and Education Technology*, vol. 13, no. 8, pp. 1251–1260, 2023.

[20] R. Mijanur, T. K. Tonmoy, S. R. Shihab, and R. Farhana, "Blockchain-based certificate authentication system with enabling correction," *Journal of Computer and Communications*, vol. 11, pp. 73–82, 2023.

[21] T. Shamsutdinova, "Application of the block-chain technology for digital diplomas: Problems and prospects," *Open Education*. vol. 22, no. 6, pp. 52–61, 2018.

[22] J. Guo, C. Li, G. Zhang, Y. Sun, and R. Bie, "Blockchain-enabled digital rights management for multimedia resources of online education," *Multimedia Tools and Applications*, vol. 79, pp. 9735–9755, 2020.

Copyright © 2024 by the authors. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited (CC BY 4.0).