Engineering Educators Bringing the World Together
2025 ASEE Annual Conference & Exposition
Palais des congrès de Montréal, Montréal, QC • June 22–25, 2025 ASEE
Paper ID #45655

Dedicated Blockchain for the Generation of Digital Certificates and Badges in Universities

Rodolfo Andrés Rivas Matta, Florida Altantic University
Dr. Jose Texier, LACCEI

Assistant Director of "The Latin American and Caribbean Consortium of Engineering Institutions" (LACCEI). Computer Engineer UNET (2002, Venezuela). Master of Computer Science, University of the Andes (2008, Venezuela). PhD in Computer Science from the National University of La Plata (2014, Argentina). Invited Professor and Researcher Universidad Nacional de Chilecito (2014-2023, Argentina). Ex professor UNET (2003-2015). The research areas are framed in Digital Libraries / Institutional Repositories / Open Science, Compilers and Interpreters, Natural Language Processing: *. Orcid: http://orcid.org/0000-0003-0176-6625 *. Google Scholar: https://scholar.google.com.ar/citations?user=kUQ1boMAAAAJ&hl=en&oi=ao *. ENTER (EngineeriNg educaTors pEdagogical tRaining): 2311001032

Dr. Maria Mercedes Larrondo-Petrie, Florida Atlantic University

Dr. Maria Mercedes Larrondo-Petrie has a Ph.D. in Computer Engineering and is a Professor in the College of Engineering and Computer Science of Florida Atlantic University. She is the Executive Director of LACCEI (Latin American and Caribbean Consortium of Engineering Institutions, a Titular Member of the Pan-American Academy of Engineering, and Director of the Organization of American States' OAS Center of Excellence in Engineering for the Americas. She serves on the ASEE International Division Board, and on the IEEE Education Society's Standards Committee and Educational Activities Committee. She was the recipient of the Duncan Fraser Global Educator Medal awarded jointly by the International Federation of Engineering Education Societies (IFEES) and the Global Engineering Deans Council (GEDC). She has been bestowed IGIP's ING-PAED title honoris causa, and iPEER (International Professional Engineer Education - Registered, Level 5). She has an h-index of 26 and an i-index of 60.

Laura Romero, Tecnologico de Monterrey

Dedicated Blockchain for the Generation of Digital Certificates and Badges in Universities

Rodolfo Andrés Rivas Matta Florida Atlantic University United States rodolforivasmatta@gmail.com 0000-0003-1461-0830	Jose Texier LACCEI United States texier@laccei.org 0000-0003-0176-6625	Maria Mercedes Larrondo-Petrie Florida Atlantic University United States petrie@fau.edu 0000-0003-2354-4986	Jose Sanchez Florida Atlantic University United States josesanchez2019@fau.edu 0000-0002-9418-0019

Laura Romero Tecnológico de Monterrey Mexico romero@tec.mx 0000-0001-9464-1295	Thomas Sorza Universidad Pedagogica y Tecnologica de Colombia thomas.sorza@uptc.edu.co 0009-0006-3261-5490	Juan Sebastián González-Sanabria LACCEI-Universidad Pedagogica y Tecnologica de Colombia juansebastian.gonzalez@uptc.edu.co 0000-0002-1024-6077

Abstract: The increasing digitalization of education and the need for secure, transparent, and efficient systems to validate academic credentials have led to the exploration of blockchain technology in higher education. Traditional certification systems are often slow, expensive, and vulnerable to fraud, which presents a significant challenge for academic institutions globally. This study aimed to design and implement a private blockchain platform using Hyperledger Fabric to automate the creation, storage, and validation of academic credentials across a global university network. The platform guarantees the integrity and accessibility of digital certificates and badges, thus ensuring secure and decentralized verification. The proposed system leverages the immutability, transparency, and security of blockchain to improve the existing certification process. The platform demonstrated significant benefits including cost reduction, improved security, and increased efficiency in the academic credential-validation process. The decentralized nature of this system allows credentials to be easily verifiable and protected against fraud. Furthermore, the solution supports the management of large volumes of academic records with improved scalability while maintaining privacy and compliance with relevant regulations. Private blockchain implementation using Hyperledger Fabric offers a robust solution to the challenges of academic credentials' validation. It addresses key benefits, such as cost efficiency, improved security, and transparency in academic credentials. However, implementation faces challenges, especially with respect to scalability, student data privacy, and legal compliance across multiple jurisdictions. Future studies will focus on addressing these challenges and expanding the adoption of blockchain technology across global university networks.

Keywords: blockchain, certificates, badges, university, Hyperledger Fabric, education

Introduction

Digitization was the major driver of this change. It also affects universities in their role as teaching and research organizations. Universities are using new technologies to change their processes. For example, they are developing simulated learning environments through virtual reality, 360° video archives, and massive open online courses (MOOCs) that support students' ability to learn independently of time and place [1], [2]. Universities also play an important role in the official recognition of these activities, achievements of students and teachers, and issuance of official documents and their evolution in the digital age.

The advancement of technology has brought about a transformation in various sectors of society, an example of which is the growing trend towards digitization of education [3]. This trend poses challenges not only in terms of teaching methods and tools but also in subsequent processes, such as the validation and certification of skills or qualifications issued by institutions. These certificates and recognitions can have a significant impact on people's lives: they can help them get the job they want or allow companies to decide whether a job candidate has the right skills. However, despite their important social role, traditional systems for certifying academic achievement are slow, complicated, expensive, and fraught with fraud [4].

Approximately 3% of the world's university degrees are fraudulent, as evidenced by the fact that, in 2023, the United States Department of Justice charged 25 people with electronic fraud in connection with the sale of 7,600 fake diplomas from three nursing schools in South Florida [5]. Similarly, in 2023, Colombia received approximately 9,000 document forgery cases mostly related to university diplomas [6]. Although solutions have been sought at the governmental level to mitigate this proliferation of fake degrees, such as Law 292 of 2022 (in Colombia), "By means of which the Public Consultation System of Higher Education Academic Degrees is created," they are not supported by resources that allow their implementation in the short term. For this reason, research has been conducted by educational institutions to find accurate and effective alternatives [7].

An alternative is digital credentials, which are documents that are considered "the digital equivalent of paper documents, plastic cards, and other tangible objects issued by trusted entities. These credentials replicate the functionality of traditional documents and offer advanced privacy and data protection features. In particular, they allow selective hiding of information from the recipient who accesses it, ensuring greater control over the disclosure of personal information. Digital credentials provide a convenient, secure, and privacy-oriented alternative to current identity management systems, both physical and digital. Their implementation can significantly improve the efficiency and security of identity verification, thereby reducing the vulnerabilities and risks associated with traditional methods [8], [9]. As a result, the creation and adoption of secure and decentralized digital certificate infrastructures based on blockchain technology have the potential to bring several benefits [10].

a) Blockchain Technology for Digital Certificates

Blockchain is an emerging technology for sharing transactional and decentralized data across a large network of trustless participants. In this sense, blockchain is considered a technology to address problems

in current certification and verification systems, considering its ability to provide traceability, immutability, transparency, and verifiability [11], [12], [13].

In contrast to traditional centralized systems (e.g., banks or centralized databases), blockchain operates on a decentralized network of computers, often referred to as nodes. Each node has a copy of the entire blockchain, ensuring that no single entity or authority has control over the entire system. This decentralization improves security and trust by eliminating a single point of failure. Despite the variety of blockchain networks and rapid development of new technologies, most blockchain networks use common core concepts [14][14]. Blockchain is a public, open, and decentralized ledger of transaction records.

The key to the interest in blockchain technology is its ability to move from a centralized data-recording system to a distributed system that ensures the immutability of information and the maintenance of privacy [15]. In a blockchain, data is grouped into blocks. Each block typically contains a set of transactions and a reference (cryptographic hash) to the previous block in the chain. This link forms the "chain" in the blockchain.

Blockchain relies on advanced cryptographic techniques to ensure the integrity and security of data. Once a block is added to the chain, modifying any information in a previous block would require modifying the data in all subsequent blocks, which is computationally infeasible owing to the decentralized and distributed nature of the network [16], [17]. Transactions on a blockchain are transparent and can be viewed by anyone on the network. Once a transaction is confirmed and a block is added, it becomes virtually immutable.

This immutability makes blockchain suitable for applications where trust and transparency are critical. The real revolution of Blockchain is that it redefines "trust" as "high-trust computing," since it is no longer necessary to trust anyone other than an algorithm. With this technology, the data created by one server can be replicated and verified by another server. It brings reliability, transparency, and security to all types of data exchanges: financial transactions, contractual and legal agreements, changes in ownership, and certifications [18].

b) Challenges of using Blockchain in Education

Higher education institutions seek to implement blockchain for certificate management, assessment of students' professional competencies, registration of non-academic activities, distribution of educational resources, management of academic degrees, and transfer of fees and credits. The benefits of using blockchain in these institutions include the ability to establish a widely accessible certification infrastructure, improve transparency and accountability, and facilitate the verification of the validity of the issued certificates. In this sense, by using blockchain, universities can automate the process of creating, storing, and verifying academic credentials, ensuring that they are easily accessible to authorized stakeholders and fully transparent, strengthening the integrity of educational and administrative processes, and contributing to more efficient and reliable higher education [18].

Although Blockchain technology offers several benefits in the education sector, there are also significant challenges to its adoption. The key issues include privacy and security. Despite the use of private and public keys to protect identities, the public nature of these keys allows transactions to be linked, compromising the privacy of users' transactions. Another challenge is the immutability of the blockchain. Once student performance is recorded, it cannot be changed, which can be problematic for institutions that must comply with data storage regulations, especially for sensitive information. Scalability is another

hurdle, as the transaction speed decreases as the number of users increases. This can make it difficult to handle large amounts of data in education. Despite these challenges, blockchain has the potential to improve the efficiency, security, and credibility of the education system by facilitating the management of credit, recognition, and payments. In addition, transparency can increase trust between students and institutions, promoting more efficient and reliable education [19], [20], [21].

c) Challenges of using Blockchain in Education

There are several solutions in the market that address the specific problem that the university network is trying to solve. Many private, multi-academic, and university solutions have implemented Hyperledger Fabric in their academic credential management and certificate validation projects. These use cases highlight Hyperledger Fabric's ability to provide private and permissioned solutions for identity management and certificate issuance in a secure and efficient manner [22], [23], [24]. The following are some of the most notable options currently available:

- Massachusetts Institute of Technology (MIT) has implemented blockchain for issuing digital diplomas using blockcerts. Additionally, they are exploring the use of Hyperledger Fabric to improve the scalability and privacy of academic records.
- The University of Nicosia pioneered the issuance of digital academic certificates based on blockchain using Blockcerts-Ethereum, enabling real-time verification.
- Sony Global Education. Sony used an enterprise blockchain platform to issue and verify academic certificates, contributing to the evolution of educational records in a transparent and secure manner.
- Open University has developed a digital credential system based on blockchain to eliminate fraud and facilitate degree verification, especially for employers.
- The University of California uses Hyperledger Fabric for academic credit verification between educational institutions to ensure a more efficient and transparent credit transfer system.
- Open Badge is an open standard for creating, issuing, and verifying digital badges based on blockchain, promoted by platforms such as Badgr and Accredible, which facilitate the validation of skills and competencies.
- The National Autonomous University of Mexico (UNAM) has researched the use of Hyperledger Fabric for identity management and supply chain control applications, focusing on improving security in academic environments.
- The University of São Paulo (USP) has implemented blockchain solutions based on Hyperledger Fabric for data management and in the financial sector, exploring its application in the academic field.
- The University of Chile has explored the use of Hyperledger Fabric for academic data management and security in administrative environments, aiming to optimize credential verification.
- The Technological University of Pereira has worked on blockchain projects focused on public administration and resource management using Hyperledger Fabric.
- The National University of Colombia has conducted research on the use of Hyperledger Fabric in blockchain, with applications in the education and health sectors, aiming to improve data management and validation.

Therefore, the objective of this study is to design and implement a private blockchain platform with Hyperledger Fabric to automate the creation, storage, and validation of academic credentials,

guaranteeing their integrity and accessibility in a network of global universities. The research question that is intended to be answered is: What are the benefits and challenges of implementing a private blockchain platform with Hyperledger Fabric for the automation of the creation, storage, and validation of academic credentials in a network of global universities?

Methodology

According to Hurtado [25], projective research seeks to propose innovative solutions to problems identified through a prior analysis process. In the context of this study, projective research was oriented towards improving traditional certificate systems through implementation within a blockchain. Through this approach, the aim is to transform the process of issuing, storing, and validating academic credentials in universities using a private blockchain platform with Hyperledger Fabric.

The objective of this projective research was to present a technological solution to a specific problem: the validation of certificates in a network of global universities. Although this research does not contemplate the massive implementation of the platform in all universities worldwide, it proposes a detailed design and proposal for the implementation of a blockchain-based system that automates the process and significantly improves security and trust in academic certificates. To this end, two major stages were defined within this methodological framework:

- Blockchain Selection
- Implementation

Blockchain Selection

The comparison of the three open blockchain platforms was interesting from the point of view of their application to the objective proposed in this research, as each platform has characteristics and advantages that may be more or less suitable depending on the specific requirements of the use case. The platforms that were considered are Ethereum, Polygon, and Hyperledger Fabric [26], [27], [28]. Owing to their unique characteristics and benefits, these platforms align with the objectives of the proposal to automate the creation, storage, and validation of academic credentials in global universities. Although there are other blockchain platforms on the market (Solana, Cardano, Tezos, etc.), the selection of these three was based on a detailed evaluation of scalability, security, costs, suitability to the work team environment, and needs of the university network. Below is a brief description of each:

- Ethereum is a public and decentralized blockchain platform that has become the most used platform for the creation of smart contracts and decentralized applications (dApps). This platform allows contracts to be executed automatically when certain conditions are met, which is key to the automation of processes, such as the validation of academic certificates. However, Ethereum's main limitations are its high gas fees and the scalability of its network, especially during periods of high demand, which could be expensive if a large volume of transactions needs to be validated continuously [28].
- Polygon, formerly known as Matic, is a scaling solution for Ethereum that improves transaction speed and reduces the costs associated with the Ethereum mainnet. By acting as an additional layer on top of Ethereum, Polygon facilitates fast and inexpensive transactions, which is ideal for platforms that require large-scale validation of academic certificates. Despite its benefits, polygon also relies on Ethereum for transaction security and is ultimately limited by the inherent capabilities of the Ethereum network [26].

- Hyperledger Fabric: Unlike Ethereum and Polygon, Hyperledger Fabric is a permissioned and private blockchain platform, making it suitable for use in enterprises and high-security environments. Hyperledger Fabric enables the creation of private blockchain networks, where one has full control over the participants, which is essential when handling sensitive information, such as academic credentials. Furthermore, Hyperledger Fabric does not require transaction fees for each operation, making it more cost-effective for handling high transaction volumes. Its flexibility and ability to adapt to the specific needs of universities make it an ideal choice for validating academic credentials within a private network of global universities [27], [29].

Therefore, the selection of Hyperledger Fabric as the primary blockchain platform is justified by several key features that make it ideal for the creation of a private network aimed at validating academic credentials. Unlike Ethereum and Polygon, which operate on decentralized public networks, Hyperledger Fabric offers a controlled and private system, in which universities and certification entities manage transactions without compromising privacy. In addition, the absence of transaction fees and flexibility makes it more efficient and scalable, overcoming the limitations of Ethereum and Polygon in terms of scalability and cost.

Implementation

Traditional certificate systems often face limitations concerning security, authenticity verification, cross-country validation, and global accessibility. However, blockchain technology has features that perfectly fit to solve those challenges. Inherently, blockchain records are safe against tampering, and proper implementations could make it accessible to everyone and ensure each actor has adequate permissions to interact with it. For example, approved universities could have permissions to add certificates to this blockchain while the general public would only perform validation of those certificates.

Clearly, the objective is to create a system that could replace the traditional certificate system, aiming to facilitate processes like transition for individuals seeking employment, further education, or having their degrees evaluated in foreign countries. The implementation must take multiple requirements into account. The product must be a flexible system that can handle various certificate types and formats to meet the diverse needs of universities and institutions. It must also prioritize user privacy and ensure that all certificates can be easily validated.

Proposed Architectures

Since the goal is to create a system that provides its actors a way to confer and validate certificates, the blockchain component is only a part of the final product. Issues like privacy and varying standards in academic certificates add challenges the system must solve. For instance, academic degrees are not considered public records. Therefore, there is a conflicting requirement of making certificates verifiable through the blockchain, maybe adding the certificates' data to the blockchain blocks, but that would make them accessible to anyone that can read the blockchain.

The research team analyzed various aspects that could affect the requirements and design of such a system. That highlighted the importance of inter-institutional collaboration, mostly if those institutions are based in different countries. Meanwhile, hands-on experimentation with the proposed technologies was necessary to identify any potential limitations or obstacles. The team initiated a straightforward architectural design that enables all users to engage directly with the blockchain; see Figure 1.

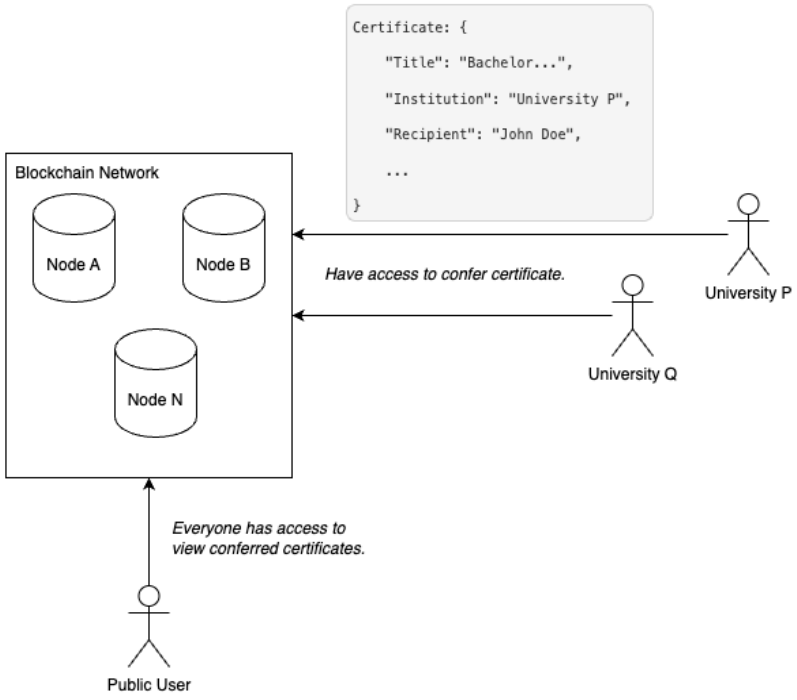

Figure 1. Initial architectural design.

The first design consisted of adding all the data of the certificates directly into the blockchain. All interactions happened directly through the smart contract. However, the certificates' fields have to be clearly defined since the deployed smart contract would not change and those fields would be the same regardless of the institution or country. The solution promptly exposed a series of deficiencies and obstacles. These included:

- Consensus Requirement: All participating institutions have to reach a consensus on various aspects of the solution; e.g., the fields that define a certificate and accessibility.
- Legal Compliance: There would be potential conflicts with the diverse legal requirements for accredited certifications across different jurisdictions; e.g., different required fields.
- Privacy Concerns: The nature of this technology creates a potential privacy concern, as all certificates added to the blockchain become permanently available public records.

The initial prototype made it possible to identify those problems and develop improved designs. Figure 2 shows the second most robust architecture. The blockchain won't be directly accessible to actors, but participating institutions can still have nodes that ensure the decentralized nature of the system. Universities can add certificates through a simple API or services that handle the certificate generation; in other words, the blockchain would be used only for record keeping. Most importantly, now the certificates' information (e.g., the recipient) is not stored in the blockchain. Instead, only the URI to the certificate, a hash of the content stored in that URI, and a signature that is useful to verify the issuer (e.g., through public-key cryptography) are stored in the blockchain.

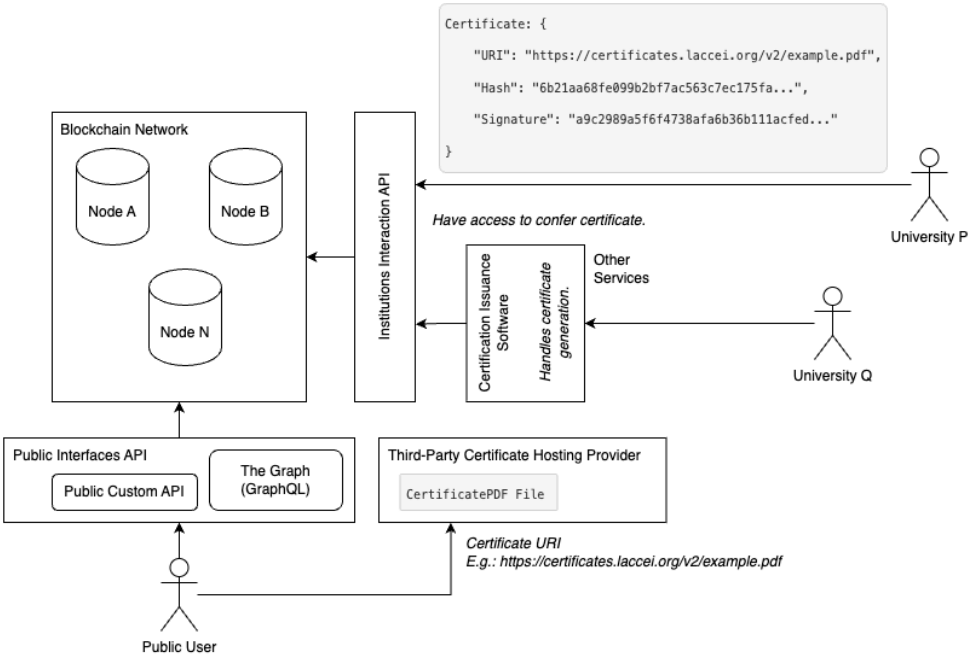

Figure 2. Second and most robust architectural design.

Privacy can be enhanced by storing the recipient's information outside of the blockchain, thereby protecting their personal data. The certificates could be stored by the same service that generated them or through a third-party service. That separate module could then handle access and permissions to proper actors. However, that may cause unnecessary restrictions stiffening the validation process again, so this area is still under active research.

Another interface was added to the design, which allows the public user to request certificates' data stored in the blockchain. The would be a service that keeps synched data of the blockchain ready to be queried. That separate module offloads direct interaction with the network, and could be scaled more easily. Third-party services like The Graph could also serve this purpose.

Initial Prototype

The first blockchain the research team analyzed was Ethereum due to its general-purpose nature, available SDKs, great documentation, and active community. The solution the team implemented on Ethereum was the first architecture. However, a major concern was cost. It became clear that Latin American countries could not afford such a solution in the long term. Even though the first prototype may have had more data to store in the blockchain, a simpler solution would still have been expensive.

```
struct Certificate {
  string issuer;
  string recipient;
  string title;
  string institution;
  string date;
}
```

Issuing a single certificate would cost approximately $5 with those limited fields. Although the cost varies depending on the networks' activity, ETH price naturally increases. The costs to publish a whole class of thousands of students becomes unbearable for countries with weaker economies. That became a major factor to move away from Ethereum. Instead, a dedicated blockchain became more realistic, and the team started exploring Hyperledger Fabric.

Shift Towards Hyperledger Fabric

Hyperledger Fabric is a permissioned blockchain platform designed for enterprise use cases. However, it seems it could adapt perfectly to solve the problem at hand. Hyperledger Fabric offers several advantages over Ethereum, including improved scalability, enhanced security, and reduced costs. Additionally, Hyperledger Fabric's modular architecture allows for greater flexibility and customization, making it an ideal choice for building a blockchain-based system for the generation and validation of digital certificates and badges in universities.

Additionally, Hyperledger Fabric has great documentation and an active community, like Ethereum. Platforms like Amazon Web Services (AWS) also offer managed deployments of Hyperledger Fabric, which simplifies the deployment and maintainability lifecycle. The team analyzed the costs and benefits of using the managed services versus deploying a blockchain from scratch in one of LACCEI's servers. Due to the limited time and qualified personnel, the team decided to use the managed service and focus the efforts in the continued development of chaincode (equivalent to Ethereum's smart contracts) to address the current issue.

The research team acknowledges that further work is necessary to fully realize the potential of blockchain technology for digital certificates and badges in universities. The team is actively exploring additional architectural designs and implementation strategies to address the identified challenges, such as privacy concerns and varying legal requirements. The ultimate goal is to develop a robust and scalable system that meets the diverse needs of universities and institutions while ensuring the security, authenticity, and accessibility of digital certificates and badges. The team is committed to continued research and collaboration with stakeholders to advance this innovative solution and contribute to the transformation of higher education credentialing.

Conclusions

This study demonstrated that the proposed private blockchain platform utilizing Hyperledger Fabric for the automation of the creation, storage, and validation of academic credentials in a global network of universities achieved its stated objectives. The implementation of this platform ensures the integrity and accessibility of academic certificates, and provides a secure, transparent, and efficient solution. The automation of processes significantly enhances operational efficiency, mitigates risks associated with traditional methods such as falsification, and facilitates expeditious and reliable access to credentials within a network of global universities.

Although the implementation faces significant challenges such as scalability, data privacy, and legal barriers, the results obtained indicate that these can be addressed through technological adaptation and implementation of inter-institutional collaboration solutions. Despite these challenges, the proposed

platform meets the fundamental requirements for establishing an efficient system to validate academic credentials in a global network.

Notwithstanding the progress achieved, this study has certain limitations that warrant consideration for future research. One of the primary limitations is the evaluation of large-scale impacts, as it is not yet feasible to predict how the system will adapt in the global context with widespread adoption. Another limitation that must be considered is that the costs of infrastructure and maintenance of the platform's features have not yet been fully delineated because of potential variations in demand that may arise as more universities join the network.

The objective of designing and implementing a private blockchain platform with Hyperledger Fabric is to automate the creation, storage, and validation of academic credentials, ensuring the integrity and accessibility of certificates within a network of global universities. However, the effective and expanded implementation of the platform will necessitate continued efforts to address the identified challenges and adapt the technology to the evolving needs of universities globally.

Future Works

Despite the progress made with the Hyperledger Fabric-based private blockchain platform for academic credential validation, there are still areas that require research and improvement. The directions for future studies are outlined below:

1. Scalability and performance: As the platform grows and the number of universities participating in the network expands, scalability needs to be assessed. The platform must be able to handle large volumes of transactions efficiently and in real-time. Integration with other platforms and the ability to support a global network of universities are essential for mass adoption.
2. Interoperability with other systems and university consortia: It is essential to investigate how to interconnect the platform with other existing educational systems at various universities. This includes integration with other academic management systems, institutional databases, and external credential-validation platforms. In addition, use cases can be explored in university consortia, such as:
    a. Issuance and verification of academic certificates
    b. Academic identity management
    c. Transparency in the recording of grades and evaluations
    d. Management of intellectual property and copyright
    e. Funding and scholarships
    f. Transfer of academic credits and recognition of degrees
    g. Access and distribution of academic material
    h. Collaboration in international research projects
    i. Decentralized grading system
    j. Management of funds and donations
    k. Audit and compliance with regulations
    l. Student and academic voting system
    m. Validation of non-formal learning experiences
    n. Creation of decentralized academic communities
    o. Peer review

3. Improving Data Privacy: Although the proposed solution improves security and transparency, privacy remains a major concern. Future developments could include the use of advanced cryptography techniques, such as Zero-Knowledge Proofs, that allow the integrity of credentials to be validated without revealing the sensitive personal information of students.
4. Expansion of the global university network: Consideration should be given to expanding the adoption of this solution within a global university network. Inter-institutional collaboration is key to its success, and ways to encourage the active participation of universities and certification bodies in the system should be explored. As networks grow, interoperability challenges and legal regulations need to be addressed to ensure that systems from different institutions communicate and validate effectively.
5. Validation of the Model: A crucial aspect for future work is to validate the proposed model. This could involve conducting interviews with university administrators and users of the platform to obtain direct feedback on system performance. It would also be useful to compare this system with other methods of validating academic credentials that are already on the market to assess the effectiveness and efficiency of the solution against existing alternatives.

References

[1] O. S. Saleh, O. Ghazali, and N. B. Idris, "Enhancing Academic Certificate Privacy with a Hyperledger Fabric Blockchain-Based Access Control Approach," *SN Comput. Sci.*, vol. 4, no. 5, p. 602, Aug. 2023, doi: 10.1007/s42979-023-02060-0.

[2] E. Wolz, M. Gottlieb, and H. Pongratz, "Digital Credentials in Higher Education Institutions: A Literature Review," in *Innovation Through Information Systems*, F. Ahlemann, R. Schütte, and S. Stieglitz, Eds., Cham: Springer International Publishing, 2021, pp. 125–140. doi: 10.1007/978-3-030-86800-0_9.

[3] L. del C. López, D. H. Vásquez, and N. L. R. Castillo, "Online education: roles, competencies and motivational strategies of university teachers," *Rev. Multidiscip. Voces América El Caribe*, vol. 1, no. 1, Art. no. 1, Mar. 2024, doi: 10.5281/zenodo.1089980.

[4] R. V. Aparco Fernández, J. A. Canchaya Esteban, A. S. Murillo García, and A. J. Robles Luna, "Modelo de implementación del proceso de emisión de grados y títulos digitales mediante el uso de la tecnología Blockchain en universidades de Lima Metropolitana," 2021, Accessed: Jan. 13, 2025. [Online]. Available: https://hdl.handle.net/20.500.12640/2161

[5] E. Whitford, "La industria de los títulos y diplomas truchos: un negocio global de US$ 7 mil millones," Forbes Argentina. Accessed: Jan. 13, 2025. [Online]. Available: https://www.forbesargentina.com/daily-cover/la-industria-titulos-diplomas-truchos-negocio-global-us-7-mil-millones-n29804

[6] C. Acosta Villada, "El plan para tumbar redes de títulos académicos falsos," El Colombiano. Accessed: Jan. 13, 2025. [Online]. Available: https://www.elcolombiano.com/colombia/asi-sera-el-plan-para-tumbar-redes-que-falsifican-titulos-academicos-CH22343562

[7] M. Al Hemairy, M. Abu Talib, A. Khalil, A. Zulfiqar, and T. Mohamed, "Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution's accreditation: UAE case study and system performance (2022)," *Educ. Inf. Technol.*, vol. 29, no. 14, pp. 18203–18232, Oct. 2024, doi: 10.1007/s10639-024-12493-6.

[8] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital Identities and Verifiable Credentials," *Bus. Inf. Syst. Eng.*, vol. 63, no. 5, pp. 603–613, Oct. 2021, doi: 10.1007/s12599-021-00722-y.

[9] I. Alamillo Domingo, "SSI eIDAS legal report: how eIDAS can legally support digital identity and trustworthy DLT-based transactions in the digital single market," *Joinup Ec Eur. Eucollectionssi-Eidas-Bridg.-Eidas-Leg.-Repor T*, 2020.

[10] G. Capece, N. Levialdi Ghiron, and F. Pasquale, "Blockchain Technology: Redefining Trust for

Digital Certificates," *Sustainability*, vol. 12, no. 21, Art. no. 21, Jan. 2020, doi: 10.3390/su12218952.
[11] M. Andreas and M. Antonopoulos, "Mastering Bitcoin: Programming the Open Blockchain." O'Reilly Media, 2017.
[12] S. Pu and J. S. L. Lam, "The benefits of blockchain for digital certificates: A multiple case study analysis," *Technol. Soc.*, vol. 72, p. 102176, Feb. 2023, doi: 10.1016/j.techsoc.2022.102176.
[13] X. Xu *et al.*, "The Blockchain as a Software Connector," in *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*, Apr. 2016, pp. 182–191. doi: 10.1109/WICSA.2016.21.
[14] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," Oct. 2018. doi: 10.6028/NIST.IR.8202.
[15] S. Nikolić, S. Matić, D. Čapko, S. Vukmirović, and N. Nedić, "Development of a Blockchain-Based Application for Digital Certificates in Education," in *2022 30th Telecommunications Forum (TELFOR)*, Nov. 2022, pp. 1–4. doi: 10.1109/TELFOR56187.2022.9983672.
[16] A. Gayathiri, J. Jayachitra, and S. Matilda, "Certificate validation using blockchain," in *2020 7th International Conference on Smart Structures and Systems (ICSSS)*, Jul. 2020, pp. 1–4. doi: 10.1109/ICSSS49621.2020.9201988.
[17] F. Kabashi, H. Snopce, A. Aliu, A. Luma, and L. Shkurti, "A Systematic Literature Review of Blockchain for Higher Education," in *2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD)*, IEEE, 2023, pp. 1–6.
[18] U. Rahardja, Q. Aini, F. Budiarty, M. Yusup, and A. Alwiyah, "Socio-economic impact of Blockchain utilization on Digital Certificates," *APTISI Trans. Manag.*, vol. 5, no. 2, Art. no. 2, Mar. 2021, doi: 10.33050/atm.v5i2.1508.
[19] M. Gottlieb, C. Deutsch, F. Hoops, H. Pongratz, and H. Krcmar, "Expedition to the blockchain application potential for higher education institutions," *Blockchain Res. Appl.*, vol. 5, no. 3, p. 100203, Sep. 2024, doi: 10.1016/j.bcra.2024.100203.
[20] R. Arenas and P. Fernandez, "CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials," in *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, Jun. 2018, pp. 1–6. doi: 10.1109/ICE.2018.8436324.
[21] J. C. Farah, A. Vozniuk, M. J. Rodríguez-Triana, and D. Gillet, "A Blueprint for a Blockchain-Based Architecture to Power a Distributed Network of Tamper-Evident Learning Trace Repositories," in *2018 IEEE 18th International Conference on Advanced Learning Technologies (ICALT)*, Jul. 2018, pp. 218–222. doi: 10.1109/ICALT.2018.00059.
[22] A. El Koshiry, E. Eliwa, T. Abd El-Hafeez, and M. Y. Shams, "Unlocking the power of blockchain in education: An overview of innovations and outcomes," *Blockchain Res. Appl.*, vol. 4, no. 4, p. 100165, Dec. 2023, doi: 10.1016/j.bcra.2023.100165.
[23] R. Kumar Kaushal, N. Kumar, and F. Flammini, "Enhancing Data Integrity in Higher Education: A Blockchain-Based Student Complaint System Using Hyperledger Fabric," *Int. J. Comput. Digit. Syst.*, vol. 16, no. 1, pp. 1387–1397, 2024.
[24] M. A. W. Saputra, D. Ochtaffia, D. Apriani, S. C. Yusfi, and M. Gori, "Blockchain Applications in Education Affecting Challenges and Problems in Digital," *Blockchain Front. Technol.*, vol. 2, no. 2, Art. no. 2, 2023, doi: 10.34306/bfront.v2i2.155.
[25] J. Hurtado, *Cómo formular objetivos de investigación*, 2da ed. Venezuela: Fundacion Sypal, 2008.
[26] Polygon, "Polygon - Web3." Accessed: Jan. 12, 2025. [Online]. Available: https://polygon.technology/
[27] Hyperledger Foundation, *Hyperledger Fabric*. (Jan. 12, 2025). Go. Hyperledger. Accessed: Jan. 12, 2025. [Online]. Available: https://github.com/hyperledger/fabric
[28] Ethereum, "Ethereum.org: The complete guide to Ethereum." Accessed: Jan. 12, 2025. [Online]. Available: https://ethereum.org/en/
[29] Hyperledger Foundation, "A Blockchain Platform for the Enterprise — Hyperledger Fabric Docs main documentation." Accessed: Jan. 12, 2025. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.5/

PRESENTACION

Fortalezas del paper

1. **Relevancia del Tema**
    - El artículo aborda un problema **crítico y actual** en el ecosistema de la educación superior: la validación segura y descentralizada de credenciales académicas.
    - El enfoque mediante blockchain, especialmente con **Hyperledger Fabric**, es técnicamente sólido y está alineado con tendencias globales en transformación digital educativa.
2. **Metodología clara y justificada**
    - Se emplea un enfoque **proyectivo** con comparación tecnológica de plataformas (Ethereum, Polygon, Hyperledger Fabric), justificada en criterios como escalabilidad, costos y privacidad.
    - Se incluye una **propuesta arquitectónica** y su evolución desde un modelo idealizado hasta una versión viable y realista.
3. **Valor práctico y aplicabilidad**
    - El desarrollo de un prototipo y la discusión de su implementación real, incluyendo aspectos técnicos como APIs, URIs, hashes y firmas criptográficas, aportan valor práctico al paper.
4. **Bibliografía extensa y actualizada**
    - Se citan más de 60 fuentes, incluyendo artículos recientes (2023-2024), reportes legales, casos de uso reales (MIT, UNAM, USP, etc.) y guías técnicas.

⚠️ Áreas de mejora / Observaciones para revisión

1. **Validación del modelo**
    - Aunque se menciona un prototipo, **no se presenta evidencia empírica ni pruebas de usuario**, ni se incluye retroalimentación de stakeholders. Incluir entrevistas piloto o simulaciones fortalecería el valor académico del paper.
    - Se recomienda clarificar si se ha hecho alguna validación funcional o técnica más allá del diseño.
2. **Redacción técnica y estilo**
    - Algunas secciones pueden beneficiarse de una redacción más fluida. Frases como *“the*

would be a service" son errores menores pero deben corregirse.

- Hay redundancia en ciertas partes, especialmente entre las secciones de introducción y antecedentes.

3. **Visualización técnica limitada**
    - Las arquitecturas se mencionan pero **no se describen en profundidad en texto** ni se explican los componentes en las figuras.
    - Se sugiere incluir leyendas explicativas más completas para los diagramas.
4. **Consideraciones éticas y legales**
    - Aunque se menciona el tema de privacidad y cumplimiento legal, **no se profundiza en normativas específicas** como FERPA (EE.UU.), GDPR (UE) o leyes latinoamericanas. Esto podría explorarse más en "Future Work".

✍️ Comentario para los autores

El trabajo presenta una propuesta sólida y bien documentada para el uso de blockchain en la validación de certificados académicos, con una elección técnica adecuada (Hyperledger Fabric) y una arquitectura evolucionada basada en las limitaciones detectadas. Recomendamos fortalecer la validación del sistema con datos empíricos o simulaciones, corregir errores menores de estilo y ampliar la discusión sobre regulación y gobernanza. El artículo tiene alto potencial para contribuir a los debates sobre credenciales digitales seguras en educación superior.