SPECIAL ISSUE

The application of blockchain algorithms to the management of education certificates

Raúl Jaime Maestre[1] · Javier Bermejo Higuera[1] · Nadia Gámez Gómez[1] · Juan Ramón Bermejo Higuera[1] · Juan A. Sicilia Montalvo[1] 🄳 · Lara Orcos Palma[1]

Abstract

Blockchain is a new application technology in many sectors and the same is true in the world of education. Therefore, there is an increasingly emerging need to research blockchain technology, as it is still taking its first steps in different sectors, such as education. This article presents a review of the state of the art of blockchain technology in the education sector, focusing on identifying the advantages, disadvantages, and challenges associated with the introduction of blockchain technology in the education sector. In addition, the implementation of a title certificate solution through blockchain technology through the BeCertify project is presented. In this solution, the development stages of the platform, the system architecture, and the operation of the API have been carried out, resulting in a platform that constitutes the first step towards a more transparent and technologically advanced way of managing the certifications of the students' qualifications.

Keywords Blockchain · Cryptographic algorithms · Technology · Digital certificates · Cybersecurity

1 Introduction

The education sector, like the rest of the sectors, continues to move towards the digital age. Technology and education are combining better and better, transforming it [1].

The adoption of technology in the education sector is a slow and difficult process. Researchers, teachers, and professionals have established different steps to support the implementation process, and in the case of blockchain technology, to implement security measures. Blockchain technology offers great potential in the area of security. In recent years, there has been a great boom and interest in the security of Information and Communication Technologies (ICT) and specifically in the Bitcoin cryptocurrency, devised by Satoshi Nakamoto [2], who indicates in the article "Bitcoin: an electronic peer-to-peer cash system" that it has provided a possible solution to transaction security. Therefore, there are different possibilities for applying blockchain in different processes and therefore it is attracting the attention of

researchers and professionals. As projects and applications based on blockchain technology grow, it is important to have access to the practice and current state of technology.

In this article, a research to understand the state of the art for the application of blockchain technology in education is presented. The objective of this article is to provide a classification and synthesized vision of current practices as well as to present the implementation of a platform for academic degree certificates based on this technology. This constitutes the first step toward a more transparent and technologically advanced way of managing Certifications of the degree of the students that have collaborated with the INITIA company in IEBS Business School. The research questions are:

- Is there evidence of the application of blockchain technology in the educational sector to solve problems or offer solutions?
- What are the specific applications of blockchain technology in the education sector?
- What are the results offered according to the study of the state-of-the-art?
- What are the results of the implementation of a blockchain-based academic degree certificate platform for the education sector?

✉ Juan A. Sicilia Montalvo
  juanantonio.sicilia@unir.net

1 Escuela Superior de Ingeniería y Tecnología, Universidad Internacional de La Rioja, Avda. de La Paz 137, 26006 Logroño, La Rioja, Spain

One of the main objectives of this article is to present the process of implementation of an academic degree certification system using blockchain technology with the start-up BeCertify. In this system, there are analyzed the different stages of development that the platform has to pass for the generation of academic degrees with blockchain technology, the system architecture a platform should have, and the operation of the REST API, present the problems that have arisen and the result of the internal management system for certification of degrees for students in an educational center.

The structure of this article is as detailed below. The current section presents the work motivation and contributions of the article in detail. Section 2 "Blockchain-based solutions for the education sector" presents important projects and research in the field related to this study. The main contribution of the article is presented in Sect. 3 "Implementation of a platform for issuing academic certificates", in which the proposed concept of the platform, the implementation of the prototype and the inclusion of the reflections and problems of the work are presented. Finally, the "Conclusion" and "Future directions" sections provide a summary of the proposed solution and some future plans.

1.1 Motivation

Most higher education institutions maintain records of their programs in a proprietary format. These databases are structured to be accessed exclusively by center staff and in dedicated online systems, therefore with little or no compatibility. In addition, most centers have their specialized system for maintaining complete student course records and preserving a data structure for information. In general, these databases are housed in a data center, with restricted access. Students can have external access to their degrees in a restricted and password-protected way, just to see the title of their program. There are different points regarding these systems, including data standardization, storage location, security, and secure sharing of title information. According to these problems, educational centres maintain the titles of their programs indefinitely.

This is done for legal reasons, depending on the policy of the country where the educational centre is. Also, in most cases, schools do not share the data of their students, not even the records of completed programs. Therefore, students may experience difficulties in demonstrating the completion of a program to another school, while retaining and demonstrating completion of the program at the previous school. This problem is even more evident in cases where the student wants to demonstrate a degree from one country to another, where there is a validation barrier at the administrative level. In addition, these registers are generally stored by different standards, making it difficult to exchange information between educational centres.

In the case that the student applies for a job and has to prove his/her qualification in a foreign country, problems arise from the centralized storage of complete records of the student's program due to its inaccessibility, and lack of standardization of student information. Title, etc. Therefore, students have to translate and validate their academic qualifications, which can be a complex, slow and expensive process.

Also, after completing their degree, sometimes, students do not have access to the academic certificate. Moreover, if a student loses it, he or she needs to reapply for a copy, which can be expensive and time-consuming.

Although there are some standards for the degree certification system, the adoption and implementation of a decentralized, reliable, and secure platform is a great challenge. There are many obstacles stemming from the fact that the academic information of the degrees is sensitive and has complex management regulations.

1.2 Contribution

To solve the aforementioned problems, we propose a platform for the management and implementation of certificates in Blockchain technology for decentralized higher education centres, called BeCertify. It is based on the peer-to-peer.

distributed network (P2P) system. This system is flexible, safe, and resistant due to its global storage and data exchange capacity. The BeCertify platform transfers the certificate of higher education degrees from the physical and analog world to an efficient and simplified version, based on Blockchain technology. The BeCertify platform provides a unified and simplified higher education degree system. Through this initiative, the researchers plan to advance and develop the BeCertify concept in other sectors.

2 Background and related works

Due to the benefits of Blockchain technology, different platforms based on it have been launched. Therefore, some of the most popular platforms are presented, focusing on those most suitable for their application in the educational sector [3].

Blockchain technology is relatively new and so is its application in the educational sector is very recent. However, there are already a large number of proposals based on Blockchain technology that improve certain aspects of the educational sector [4].

2.1 Blockchain technology

Blockchain technology and digital currencies, also called cryptocurrencies, are key applications of distributed accounting technologies that became a star issue in 2016 and 2017. Powered by their potential to revolutionize multiple industries, and the increased value of digital currencies, particularly Bitcoin, this technology has become a top strategic priority for some companies [5].

Considering the potential of technology to reduce costs, create capital, improve trust systems, minimize inefficiencies, and radically transform business models [5], it is not surprising that multinationals research and reap the benefits of this technological innovation.

Blockchain technology is similar to a shared database. A "distributed ledger" is a special type of ledger in which transaction logs are distributed across a network that spans multiple locations. Each participant in the network has an identical copy of the ledger. As a result, when a change is made to the general ledger, it is spread and reflected on all copies held by network participants (the speed of this process depends on the type of network, however some networks require several seconds or even minutes to extend and reflect the changes). Distributed books maintain the security and precision of transactions by implementing cryptographic protocols and signatures to control access and permissions of the shared book. Access control rules are generally agreed upon and applied by the network [6].

This special type of distributed ledger supports the Bitcoin cryptocurrency. The key feature of a blockchain is that it employs a data structure where transactions are organized and grouped into a block, as can be seen in Fig. 1.

Like [7] comments each block is linked or linked, that is, chained, along with a previous block using a hash cryptographic function. Therefore, each block that is added to the chain carries an encrypted reference to the previous block. This reference is part of the mathematical problem to solve to add the following block to the network and the chain [2]. Part of the solution to this math problem is to solve random numbers called "nonce."

The "nonce" combined with other data, such as the size of the transaction, using a mathematical algorithm creates the fingerprint that transforms an arbitrary block of data into a new one of fixed length using the hash function.
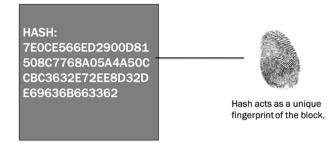

Fig. 2 Hash configuration (ID of a Block in a Blockchain)

As it is encrypted, it makes it secure against attacks on confidentiality and integrity. Each hash, as can be seen in Fig. 2, is unique and has to face certain mathematical and cryptographic conditions. Once the above is done, the block is completed and added to the Blockchain. To manipulate each previous block, it is necessary to remember the cryptographic puzzles, which have been impossible until the date [2].

Blockchain networks are classified as open or closed, depending on how they approach their security and threat model. Open Blockchains, also called public Blockchains without permission, are considered untrusted or less trusted environments because anyone, including hackers, can join the network. As a result, it is an incentive mechanism that rewards honest behavior among participants. This is done to preserve the integrity of the Blockchain network. An is Bitcoin, where so-called miners are rewarded for their effort by participating in the profits of carrying out a transaction [8].

On the other hand, closed or private Blockchains networks operate in a trustworthy environment and are considered relatively more secure than public Blockchains. The participants are known, and this eliminates the need to encourage their honest behavior [8].

An example of a private Blockchain is the custom-made Blockchain for a company, where participants do not need incentives because they share the same general objective, for example, tracking the company's supply chain. Here, participants must be held accountable through legal terms and conditions (external to the Blockchain) and encouraged to behave honestly to avoid legal repercussions [9].

Fig. 1 Blockchain

Therefore, Blockchain technology is considered the key to solving scalability, privacy, and reliability problems in several areas [10]. In other words, a Blockchain network is a distributed digital ledger that allows registering and exchanging information by a community of users in which each member keeps a copy of the information, and any update has to be validated collectively [2].

This technology is a self-regulating, auditable, tamper-proof, trustworthy system that does not need third-party intervention to execute its computational processes [11]. This database is encrypted and serves to store irreversible and incorruptible information, it allows people who are not related to each other to reach a consensus on a particular transaction or event without the need for an authority to control it [4].

Another example of the use of this technology is provided by Abba Garba et all in [12]. This paper presents the design and implementation of a blockchain-based domain authentication scheme with privacy-preserving features for mobile, browser, and IoT devices. In addition, a comparison with other authentication methods is included. Its main advantages are its storage capacity and low bandwidth for authenticating certificates.

Another use of technology in the health sector, specifically for use in the fight against the current COVID-19 pandemic, is presented in [13] which proposes a blockchain-based platform that can provide pandemic research data sharing while preserving data privacy.

Therefore, Blockchain technology is increasing in popularity because it exhibits a series of security properties that make it useful in various applications. The technology is implemented in use cases and applications where the participants do not necessarily trust each other or prefer to reduce their dependence on other third-party service providers and intermediaries [8].

2.2 Blockchain-based solutions

In Spain, the UOC (Universitat Oberta de Catalunya) established the OpenDCert project, (decentralized application for academic certificates), shown in Fig. 3, which was developed for a Final Degree Project where the public version uses one of the test networks (Rinkeby) of the Ethereum Blockchain [14]. The application is designed to enable training entities (schools, universities, training centres, etc.) to manage student certificates safely and without intermediaries, showing a management alternative based on this technology. The application is designed to store any private data, and public keys that are associated with each type of user (organizations, students, and administrators) are always used, as indicated in Fig. 3. The functionality of organizations or training entities is to manage certificates of students associated with a public key. Students can only consult, download and share the certificates and, on the other hand, the administrator validates that the entities are correct [14].

Another initiative can be found at UNIR (Universidad Internacional de La Rioja) and the Certiblock project for the issuance of academic degrees and certificates safely and efficiently, which also enables these documents to be available to other universities or companies [15]. That is, issuing academic certificates with Blockchain guarantees efficiency, security, and accessibility, where all interested parties can access the information and the title, which once
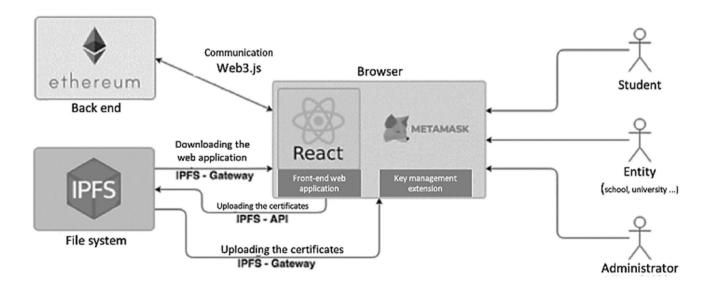

Fig. 3 Proyect OpenDCert [14]

it is registered in the blockchain, is unalterable. The title is always available within the Blockchain itself, but it is also a validation mechanism so that students, regardless of whether the institution disappears or not, can demonstrate the veracity of the certificate. For this, the entity responsible for issuing the certificate registers the smart contract on the network and issues a certificate for the student with an ID. An attempt to create an ecosystem is made, in which all universities participate in a distributed database in which they are shared, also with companies that want to check whether a degree issued to a candidate or worker is real or not [15].

The reference article [16] presents the Blockchain for Education platform for issuing, validating, and sharing digital certificates. According to the authors, the main advantages of this platform are the ability to store immutable and decentralized digital certificates, the existence of a service that verifies the authenticity of the certificate, and the secure storage of the identity of the organization. Platform-issued certificates are based on the Mozilla Open Badges specification and allow for viewing or validating revoked certificates.

The Massachusetts Institute of Technology (MIT) and the company Learning Machine have developed another university project called Blockcert [17] [18] [19]. The main objective of this initiative is the development of an open standard available to any educational institution that issues certificates. It provides open-source libraries, tools, and mobile apps. This system is currently implemented at MIT, the University of Nicosia and the University of Birmingham.

Another one can be found at IEBS Business School which is starting the transformation of its business model to a Blockchain education company with the help of the startup BeCertify. The business model of the company want to develop it is based on a Blockchain infrastructure. In summary, it plans to break into the sector, by improving its services, using Blockchain technology, and reating an incentive system that rewards the best teachers and the best students. The platform wants five essential elements: students, teachers, workers, advertisers, and sponsors to push through the
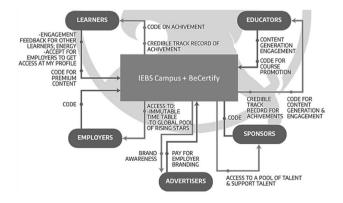
Blockchain, as Fig. 4 indicates. The personal benefits of using the platform are:

- Students: they will receive paid tokens to learn, they will benefit from learning minutes, they will have a history of achievements and they will get social comments from other students and teachers, in addition to having access to work. Opportunities are created through networking.
- Teachers: they will receive paid tokens to teach, and, through their personal history, they will be able to become star teachers. At the same time, they will also be able to earn tokens for helping students with fewer resources.
- Workers: their main advantage comes from their access to the records and achievements of the training campus. They will be able to follow the achievements of potential candidates and even build promotion programs.
- Advertisers: they may create brand recognition for supporting an IEBS program or programs.
- Sponsors: they can sponsor individual talents or courses from the available catalogue.

Kanan et all, in reference to article [20] present SmartCert as a Blockchain-based platform for issuing and verifying the authenticity of academic degrees and digital certificates implemented on Ethereum. For this purpose, it implements the cryptographic services provided by this technology. The platform is implemented at the University of Al-Zaytoonah.

Another initiative is the network CRUE—ICT. The CRUE—ICT project is made up of a group of private and public Universities in Spain (the University of Jaén, University of Extremadura, Polytechnic University of Madrid, Public University of Navarra, Polytechnic University of Valencia, Complutense University of Madrid, University of Murcia, University from Alicante and the University of Santiago de Compostela), each of which has its node, and works to connect to the European BLUE network [21].

Other higher education institutions that have adopted Blockchain to certify degrees are the ISDI business schools, ESADE, ESIC, and the Carlos III University of Madrid, which carry out-degree certification with the start-up Smart-Degrees, in addition to a mobile application through which students can manage or share the certificates with work platforms and companies [22].

On the other hand, the 3 Chain CEU (Universities in Madrid, Valencia, and Barcelona), both members of ALAS-TRIA [23], are entered into the Ibermatic Chain Talent platform.

Another initiative born in the framework of the European Union is EduCTX [24] developed to digitize the European Credit Transfer and Accumulation System (ECTS). The platform implements a system to process, verify and monitor ECTX tokens as academic credits. The users of this platform

Fig. 4 Business model (Blockchain infrastructure)

are students and universities and higher education organizations. Each institution has its EduCTX address. The main feature of this system is the multi-signature authorization capability of the different actors involved in the process provided by the open ARK Blockchain, distributed P2P network architecture and its performance in terms of concurrent data processing of multiple users.

Other similar solutions in this field found in the literature but for which not enough information is available are RecordsKeeper [25], TrueRec [26], Sovrin [27], Taiwan Ministry of Education [28] and UZHBC [29].

In summary, Table 1 makes a comparison of the most important projects and their main characteristics. As we

have safely and efficiently catalogued the seen in the article, the academic records of a person, such as degrees, are data stored in databases of various education providers, and students or graduates do not have the authority to manage their information. Furthermore, another person does not have access to modify or even view these records. But in a context of a greater internationalization of education and work, with the increasing mobility of students and graduates, it is essential to have easy access to the registration of degrees on a personal level.

Other studies identify the challenges related to the recognition of degrees, certificates, and diplomas issued by foreign education providers, taking into account the

Table 1 Comparison of the projects

	Institutions	Blockchain	Network type	Consensus algorithm	Type of consensus
Certiblock	UNIR	Ethereum	Public	Proof of Work (PoW)	Proof of work (51%)
OpenDCert	UOC	Rinkeby	Public	PoW	Proof of work (51%)
Blockchain for Education	Fraunhofer, University of Luxembourg	Ethereum	Permitted Private	– *	– *
Blockcert	MIT, University of Nicosia, University of Birmingham, South Ural State University, University of Rome and University Fernando Pessoa	Ethereum, Hyperledger, Bitcoin	PublicPermitted Private	Proof of Authority	– *
BeCertify	IEBS Business School	Europe Chain	Permitted Private	PoW	Proof of work (51%)
CRUE	Jaén Univ., Extremadura Univ., etc	BLUE	Permitted Private	– *	– *
SmartCert	University of Al-Zaytoonah	Ethereum	Public	– *	– *
Smartdegrees	Carlos III Univ	Quorum	Permitted Private	QuorumChain	Red T: QuorumChain Red B: PoW, PoA e IBFT
Chain Talent	CEU	Red T: Quorum Red B: Hyperledger Besu	Permitted Private	Red T: QuorumChain Red B: PoW, PoA e IBFT	Red T: Majority vote (BFT / RAFT) Red B: Proof of work (51%), etc
EduCTX	University of Maribor BRNO University of Technology, Sarajevo University	ARX	Public	Proof-of-Stake (PoS)	Distributed PoS
RecordsKeeper	– *	RecordsKeeper Open-source	Public or Private	PoW Proof-of-Existence (PoE)	– *
TrueRec	openSAP	Ethereum	Public	PoW	– *
Sovrin	– *	Ethereum	Public Permissioned	Byzantine fault-tolerant (BFT)	Plenum an enhancement of RBFT
Taiwan Ministry of Education	Southern Taiwan University of Science and Technology	Ethereum	Permitted Private QR code	– *	– *
UZHBC	University of Zurich	Ethereum	Public	– *	– *

*Not available information

dangers of counterfeiting. They developed some recommendations to ensure that a document is not fraudulent [30]. One of these recommendations is a complete and reliable system to record, store and retrieve educational information, such as degrees, certificates, diplomas, educational credentials, training, etc. Among other purposes, this type of system would help to prevent fraud, ensuring, data management and access to third parties (other universities, recruiters, or employees), even between different countries.

2.3 Benefits of blockchain technology in the education sector

Blockchain technology has not yet realized its full potential and could become an important part of educational systems. Some of the benefits of adopting this technology in the field of education are the following [31]:

- Decentralization: considering a distributed peer-to-peer architecture over a centralized one, improves fault tolerance, by eliminating the central points of failures and bottlenecks.
- Scalability: allows the elimination of situations in which one or more entities control the storage and processing of information of a large number of people.
- Reliability: the information can remain unchanged, immutable, and distributed overtime on the Blockchain. Any participant in the system can verify the authenticity of the data and ensure that it has not been altered.
- Reduction of administrative costs and reduction of bureaucracy.
- Security: information and communications can be secure when considering Blockchain transactions, based on cryptographic protocols. Thus, for example, Blockchain offers the potential to make title records more secure.

2.4 Limitations of the application of blockchain technology in the educational sector

Several problems in the implementation of education applications based on Blockchain technology have been detected. Mainly, these revolve around compliance with data protection laws, ownership of data, and the authenticity of data sources.

Latency time is another limitation in Blockchain technology because the transaction can a lot of time. Increased storage capacity due to data redundancy, as each node has a copy, could also be a technology adoption problem. In addition, some publications reveal a major security problem in the proof of work (PoW) consensus algorithm, called the "51% attack" [8].

On the other hand, it is important to mention that the adoption of Blockchain technology in the educational sector makes it necessary to solve several legal problems [32]: for the determination of who is responsible for the treatment -data controllers- as well as the viability of fulfilling the obligations that correspond to them, they would anonymize the personal data, or, finally, the exercise of some subjective rights related to the data. As noted above, the compatibility problems with Regulation (EU) 2016/679, of April 27, 2016, which entered into force on May 25, 2018, are greater in the chains of public blocks that are private and have not been definitively resolved either by the laws of some countries or by the community data protection authorities.

3 Implementation of an academic certificate issuance platform

This section describes the development of the INITIA company in the BeCertify project for the IEBS Business School client and the management and implementation platform for degree certificates in Blockchain technology for decentralized higher education centers.
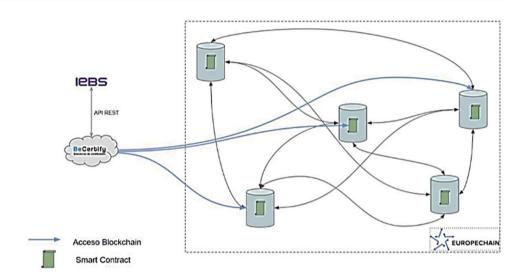
INITIA and IEBS Business School believe that digital transformation is the key to seeking competitive advantages and, thus, to be able to explore new business opportunities. In this context, INITIA has become a technology provider for IEBS Business School, to detect some of the opportunities that exist in the market and accompany it in their materialization.

This section includes the services necessary to carry out the implementation of a certificate issuance platform based on Blockchain technology, which allows IEBS Business School to guarantee the authenticity of the degrees it issues.

One of IEBS Business School's needs is to focus on issuing certified academic degrees in Blockchain technology. These certificates can be managed from mobile applications and shared with recruiting companies and social media platforms like LinkedIn, in a way that guarantees the inviolability of the title.

INITIA presents to the IEBS Business School a solution with the BeCertify-based. BeCertify is a digital certification platform based on Blockchain technology through the EuropeChain network, a technology derived from EOS, as opposed to Bitcoin or Ethereum. This network allows great scalability while keeping costs low and complies with European data protection regulations.

Fig. 5 Architecture developed in phase 1
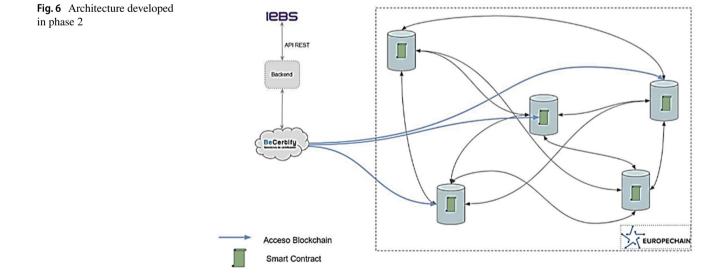

3.1 Platform development phases

The development of the platform has been addressed in three different phases. The first "Phase 1" consists of a proof of concept. The objective of this phase is to demonstrate that the solution is valid to meet the objectives of IEBS Business School and to demonstrate the technical robustness of the platform.

It is implemented through a technical infrastructure necessary to create the certificates and host them in EuropeChain. In addition, a REST API is provided to IEBS Business School to connect to the Blockchain network and internal business processes when certifying degrees and checking their validity. The tasks, as shown in Fig. 5, carried out were:

- Deployment of the Smart Contract.

- Management of the private key.
- REST API creation:

  - Certification registration service: Service that allows IEBS Business School to create a new certificate. Its main argument is the certificate code, and it returns a HASH code to identify the certificate within EuropeChain.
  - Certification consultation service: Service that allows IEBS Business School to validate the authenticity of a certificate. The HASH code is accepted and returns a boolean indicating the authenticity.

Phase 2 consists of developing the minimum viable product. In this phase, a services module is developed on the Blockchain layer that allows IEBS Business School to manually manage the creation of certificates. This tool allows, in

Fig. 6 Architecture developed in phase 2

the future, to expand the business logic necessary for any operation with smart contracts, betting on a modularized cloud architecture that allows a scalable and maintainable solution. The tasks that were carried out during this phase were:

- Management of status of a title (pending certification, certified, expired, etc.).
- Linking metadata by certificate (centre, degree, student, date, issue, etc.).
- Control of access to services.
- Collect and analyze usage statistics.
- Performance reports.

In the architecture developed in "Phase 1", the BackEnd component is added, as shown in Fig. 6, which isolates the service layer of IEBS Business School's business specialists, offering a friendly interface aligned with its objectives.

Phase 3 consists of the complete certification of the degree and integration with business processes. In this phase, the suitability of the platform and the correct integration in the dynamics of degree management are validated. It is important to consider the evolution of the solution to seek greater synergies.

The scope of the third phase is defined during service. The possibilities that can be developed according to INITIA are:

- Complete certification of the degree:

  - The creation of partial certifications is allowed, which certify that the student has achieved certain milestones in their training itinerary (passing exams, evaluating assignments, doing practicals, etc.).
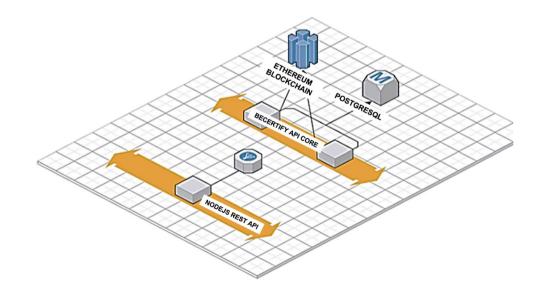
  - Once all the necessary certifications have been collected, the certification of the student's title can be issued.
  - This solution allows IEBS Business School to guarantee the authenticity of the degree and the merits of the students.

- Integration with business processes:

  - The corporate systems of IEBS Business School can be analyzed to perform automatic integrations of the REST API.
  - The technical nature of the integration has to be defined, and the solutions proposed must have to be compatible with the technical ecosystem of IEBS Business School.

3.2 System architecture

At this point, the main characteristics of the technical solution that gives service to IEBS in its issuance of digital certificates are collected. The architecture diagram, as shown in Fig. 7, shows the main components of the system, bearing in mind that BeCertify is a key element and isolates all the complexity of access and management of the blockchain network.

The description of the different components is determined in the architecture diagram and details the following responsibilities (IEBS Business School management module):

- Module deployed in IEBS Business School systems.
- Aims to:

  - Encapsulate the use of BeCertify.
  - Manage BeCertify credentials and authentication.

Fig. 7 Architecture diagram

- Host customized business logic for IEBS Business School as a result of your business requirements or your corporate systems.
- It offers an API in RESY format to be consumed from IEBS Business School corporate systems.

- Technology:

  - Node.js in version 8.
  - Express as a development framework.

3.3 Framework of Blockchain development

At this point, the Blockchain Development Framework concept is presented within the scope of the BeCertify implementation project as a component in the issuance of certificate certificates based on Blockchain technology for certification of degrees at IEBS Business School.

In the project, to implement the BeCertify solution at IEBS Business School, as Fig. 8 shows, a technological base called the IEBS Blockchain Framework has been developed. It is a set of components and tools useful for implementing solutions and processes based on Blockchain technology.

The components of the IEBS Frawework blockchain would be:

- Blockchain framework:

  - Node.js application that brings together the logic necessary for the current and future use of several Blockchain technology solutions.
  - This application can be evolved according to the needs, to incorporate new functionalities and access to new services based on blockchain technology.

- External service:

Fig. 8 Framework Blockchain

- Market service that provides IEBS Business School with a concrete value proposition based on Blockchain technology.
- These external services are responsible for accessing the Blockchain network directly.

- Internal Service:
  - Development services at IEBS Business School to incorporate functionalities based on Blockchain technology into the organization that does not depend on the service of third-party companies.
- The services has to be designed to be integrated through the REST API.Corporate systems:
  - Tools and systems that serve IEBS Business School in its processes and business.

The scope of version 1 of the Framework, as Fig. 9 shows, includes the necessary mechanisms for the issuance of degree certificates.

However, with the implementation of Blockchain technology with Node.js, the Framework is prepared to carry out the necessary integrations with all kinds of services, both internal and external, products and tools of blockchain technology, as Fig. 10 shows.

3.4 Use of the API REST

This point aims to clarify the concepts related to the consumption of the IEBS Business School API to create certificates based on Blockchain technology for their degrees, as shown in Fig. 11. Certificate management functionalities are available through a REST API. It is important to consider the following concepts when using it:

- Endpoint: URL through which it is possible to access the method.
- Operation: Information access method (GET, POST, PUT, PATCH or DELETE).
- Body: Arguments of the method. Typically, this is information that must be processed by the API.
- Status and error code HTTP: Success or failure in executing the method.
- Answer: JSON file with the data returned by the method.
- The methods available in the API are as follows:
- Create-Cert: Method dedicated to the creation of a new certificate in BeCertify and its registration in the Blockchain network, as Fig. 11 shows.

  - Endpoint: / api / v1 / certificate
  - Access method: POST
  - Headers: Not necessary
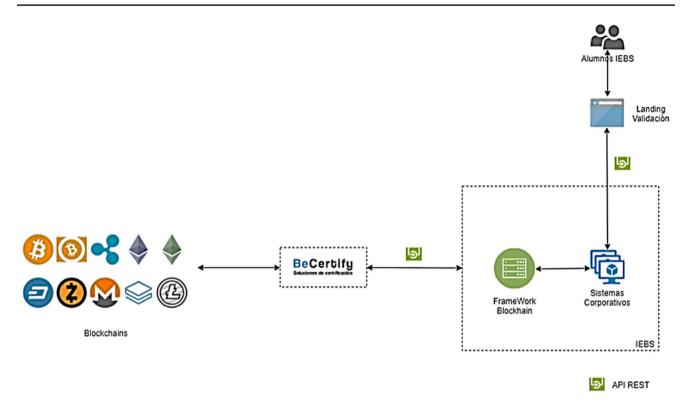 - Body: JSON with the following arguments:

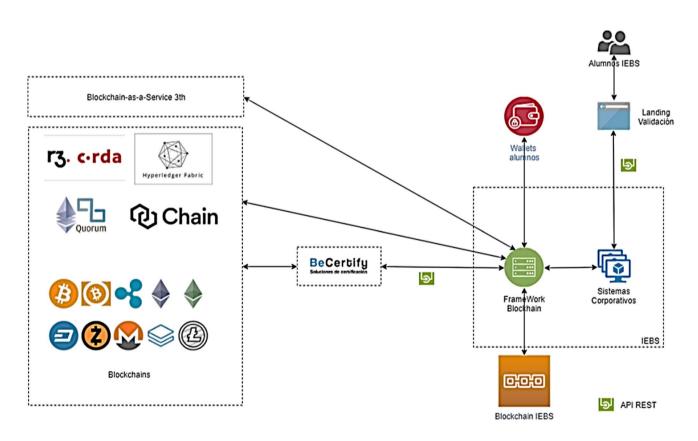**Fig. 9** Version 1 of the Blockchain Framework

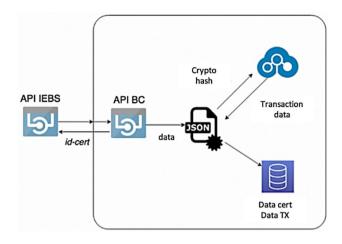**Fig. 10** Version of the Blockchain Framework

Fig. 11 Creation of the certification

```
{
"Id": "title identifier"
"Name": "Name of the degree"
"Student": "student's name",
"Student_suername": "Student surnames"
"Director": "Name of teacher or director",
"Hours": "Hours of the program"
}
-          Answer: JSON with the following data:
{
"Id": "unique certificate id",
"Hash_transaction": "id of the transaction in
Ethereum blockchain",
"Hash_proof": "unique hash receipt of the
transaction saved in Ethereum"
"Issued": "DateTime certificate issuance on
blockchain"
"Name": "Name of the degree"
"Studen": "student's name",
"Student_suername": "Student surnames"
"Director": "Name of the teacher or director",
"Hours": "Hours of the program"
```

- Verify-Cert: Method dedicated to verifying the validity of a certificate and its associated data.

  - Endpoint: / API / v1 / certificate / {certificate_id}
  - Access method: GET
  - Headers: Not necessary

- Body. JSON with the following arguments: unique ID of the certificate
- Answer. JSON with the following data:

```
{
"Id": "internal id",
"Hash_transaction": "id of the transaction in
Ethereum blockchain",
"Hash_proof": "unique hash received from the
transaction saved in
Ethereum"
"Issued": "DateTime certificate issuance on
blockchain"
"Name": "Name of the degree"
"Studen": "Student Name",
"Student_suername": "Student surnames"
"Director": "Name of the teacher or director",
"Hours": "Hours of the program"
}
```

The access and consumption of the different Endpoints of the REST API, as Fig. 12 shows, depends on the technology that is being used for development. They can be developed in some modules and components of the most common web technologies, such as the following:

- JavaScript: Fecth API or JQuery AJAX
- Ruby: Net:HTTP class
- Python: Requests Module

For validation and testing, all these tools and components can be accessed using the POSTMAN graphical tool.

3.5 Certificate of the degree for the student of the IEBS Business School

Once all the development of the REST API has been completed, the internal IEBS Business School system was developed. In the internal system, a specific section is created where the different fields are generated to connect to the API and generate the BeCertify JSON file, as Fig. 13 shows.

Once the internal system develops, the diploma creates, and it can be consulted from the student's profile. In this section you can verify the title, the course completed, the date of issue and a button has been created to verify the diploma, as Fig. 14 shows.
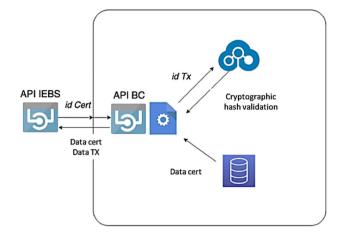
Fig. 12 Certificate verification

```
{
    "id": "86163d7a-bff8-489a-b4c8-d126df0cd35f",
    "tx_id":
"0x168d7dc1fa635919a96d518ca6f758cc8593e6e
193601ab4ce3026fcff71ef44",
    "ethercan_url":
"https://etherscan.io/tx/0x168d7dc1fa635919a96d5
18ca6f758cc8593e6e193601ab4ce3026fcff71ef44"
,
    "target_has":
"2f75ef69d9f6e5ce4e29ff2a056ef0b41d064463523
d5b318039599837a0f281",
    "name": "Blockchain for techniques",
    "hours_program": 8,
    "student": "Galilea Rodriguez",
    "student_surname": "Galilea Rodriguez",
    "expedition": "2019-10-29",
    "director": "Miguel López"
}
```

When the diploma is verified, as Fig. 15 shows, the digital credential with the Blockchain ID can be consulted. On the same verification screen, the JSON test file that has been created in the title accreditation circuit can be downloaded (Fig. 16).

Ten (10) tests were performed for the issuance of titles generating, for example, the following JSON file:

In order to test the system, 34 issues of titles were launched. In 6 of them, an error occurred in which it appeared that the UUIDS was not valid, and the rest was valid information. This error occurred when validating UUIDS with the 'PostgreSQL' driver used. The identified problem was solved, and the tests were subsequently re-run without the error appearing.

Fig. 13 Certification creation system

Fig. 14 Public certificate

Fig. 15 Verification screen

4 Discussion

The research presented in this article consisted of the implementation and development of a BeCertify certification and degree issuing platform for educational centers based on blockchain technology and a distributed peer-to-peer (P2P) network system. The tests were carried out and developed in a real environment provided by a higher education center.

All stakeholders (the educational institution, the student and the company) can benefit from a system for issuing and managing the certification of higher education qualifications that is decentralized, reliable in terms of the security it provides, easy to use and relieves administrative burdens on management staff.

The BeCertify platform makes it possible to move the issue and management of degree certificates from a physical and analog version to a much more efficient and simplified digital version, thanks to the use of disruptive

```
{"name":"StatusCodeError","statusCode":500,"message":"500 - \"ValidationError at /api/v1/certificate
[\\\"'f986f45d-3c25-4c8b-8850-78ea7db9be80' is not a valid UUID.\\\"]

Request Method: POST
Request URL: http://apis.becertify.io/api/v1/certificate
Django Version: 2.2.2
Python Executable: /opt/python/run/venv/bin/python3
Python Version: 3.6.8
Python Path: ['/opt/python/current/app', '', '/opt/python/run/venv/local/lib64/python3.6/site-packages', '/opt/python/run/venv/l
'/opt/python/run/venv/lib64/python3.6/site-packages', '/opt/python/run/venv/lib/python3.6/site-packages', '/opt/python/run/venv/
Server time: Mon, 3 Feb 2020 17:14:40 +0000
Installed Applications:
['django.contrib.auth',
 'django.contrib.contenttypes',
 'django.contrib.sessions',
 'django.contrib.sites',
 'django.contrib.messages',
 'django.contrib.staticfiles',
 'django.contrib.admin',
 'crispy_forms',
 'allauth',
 'allauth.account',
 'allauth.socialaccount',
 'rest_framework',
 'rest_framework.authtoken',
 'becertify_core.users.apps.UsersConfig',
 'becertify_core.issuers.apps.IssuersConfig',
 'becertify_core.certificates.apps.CertificatesConfig',
 'compressor',
 'debug_toolbar',
 'django_extensions']

Installed Middleware:

['django.middleware.security.SecurityMiddleware',
 'django.contrib.sessions.middleware.SessionMiddleware',
 'django.middleware.locale.LocaleMiddleware',
 'django.middleware.common.CommonMiddleware',
 'django.middleware.csrf.CsrfViewMiddleware',
 'django.contrib.auth.middleware.AuthenticationMiddleware',
 'django.contrib.messages.middleware.MessageMiddleware',
 'django.middleware.clickjacking.XFrameOptionsMiddleware',
 'debug_toolbar.middleware.DebugToolbarMiddleware']




Traceback:


File \\\"/opt/python/run/venv/local/lib64/python3.6/site-packages/django/db/models/fields/__init__.py\\\" in to_python
  2337.                return uuid.UUID(**{input_form: value})
```

Fig. 16 Error UUIDS no valid

blockchain technology. This technology enables globalization and scalability of the solution, as well as eliminating the problems that have arisen over the years regarding the veracity of the certificates issued.

It is an example of the benefits of this technology. It is also a major breakthrough in the field of education, as it allows verification of students' tenure at an educational institution and ensures that they are prepared for the world of work. In addition, value is given to schools by providing them with a quick and efficient mechanism to verify the qualifications of a student.

The intention of the BeCertify initiative is not to change and transform the system of qualification certification established by the different countries, but to improve transparency and automation of the administrative processes related to the issuing and management of certificates and qualifications in schools. Therefore, schools would be able to use this certification and degree issuing platform simultaneously with their management processes.

Using a platform such as BeCertify has several advantages. Primarily, it allows companies the possibility to verify the academic qualifications of their future employees in a

transparent way. Educational institutions get a decentralized and transparent way to validate qualifications. The platform gives the possibility to detect and prevent degree fraud. Therefore, the need for a more complex verification process can be avoided. In addition, students are given a system that is transparent and allows instant verification of the completion and awarding of the degree of the program they have completed at an educational institution.

The system solves the problem of obtaining access to data related to students or graduates, which is often stored in educational institutions in particular databases that are not accessible or in paper documents. Blockchain technology solves this problem while allowing it to continue as "open data".

The platform has been implemented in an educational center, which has allowed the analysis and debugging of any type of error, both on the technical and conceptual side. It is currently in the expansion phase to other educational centers.

The model has been materialized through the implementation of a functional system that has obtained positive results in the tests carried out. One of the main characteristics of the proposed model is its wide range of applicability to any educational institution that prepares students and has to issue a certification degree. It allows to check for sure that the competences have been achieved by the student and, what is more, to be able to guarantee that the preparation of these studies is in accordance with the qualification awarded by an educational institution.

The research also includes specific assumptions and limitations. The first deployment of the platform has been carried out at the first collaborating center, IEBS Business School. The platform presented several problems during its implementation and development. In the beginning, only a few nodes were part of the network, which could pose a security risk. However, over the course of its implementation, the number of nodes increased, which improved its security. Other problems are related to the storage and protection of schools' private keys.

It is necessary for all educational institutions to protect their private keys, credentials, signatures, etc. It may happen that a student loses his or her private key and is therefore unable to prove possession of an educational institution's degree. In this case, the student could request the school to send a new blockchain address after verifying their records. For added security, each stakeholder on the BeCertify platform could be issued a multi-signature, multi-level address, ensuring that an address will work even if one of the keys is lost.

In relation to data privacy and GDPR compliance, IEBS Business School's data treatment managers and data protection officers were appointed, personal data was anonymized, public and private keys were used, and security measures were included to protect the storage and private keys of all members based on the risks identified. On the other hand, Blockchain cannot guarantee the privacy of transactions due to the risk of data leakage through frequent updates or the possibility of linking user transactions to their publicly available public key. In the case of BeCertify, the latter risk is lower as it is a private network to which not all members of the public have access.

From the study of the art, it can be concluded based on Table 1 that the number of projects like the one presented in this article is growing, as well as the number of organizations involved and their mutual cooperation to create better applications of blockchain technology. The launch of blockchain-based platforms in the area of education has been studied, most of them presented in this article.

It is difficult to see in which direction and to what extent technology will provide a solution to the new proposals for daily implementation and adaptation. Currently, there are many challenges in scalability, security, and implementation of different consensus algorithms. One of the future lines of research proposed in this article is a comparison of the performance of the two most widely used consensus algorithms in use today.

The potential for the application of this technology in the field of education is unlimited considering the value of the secured data and the future functionalities it can provide. The possibilities of blockchain technology have not yet reached their full potential, but decentralization, security, and independence are becoming more and more valued among educational institutions that increasingly value the authenticity and credibility of certified data.

This article opens up the possibility of exploring the potential of blockchain technology in other areas of the education sector and extrapolating it into the creation of a system for acquiring students' skills and demonstrating them in the labour market.

5 Conclusion

This article presents an implementation model for certification and degree issuance in open higher education, based on Blockchain technology, which certifies the acquisition of competencies by students trained in educational institutions.

Due to the benefits of this technology, various Blockchain-based platforms have been launched and various applications have been developed in many diverse areas, including education, some of which are presented in this document.

Blockchain technology opens up a new approach to education that expands the possibilities of protecting users' data and guarantees the authenticity and security of various academic records, transcripts, and certificates. With

decentralized access to that kind of valuable information, it becomes truly independent like its senders and allows open and secure access.

This first approximation of the model has materialized in the form of the implementation of a platform. This implementation has been verified and validated, and the system is currently in production. Until its definitive implementation at the end of 2022, the errors detected have been progressively solved and improvements in its functionality have been developed.

6 Future directions

As the completion of the implementation is near, we consider new lines of future work:

- To create a model that allows the comparison of training entities dedicated to training students in the same professional skills.
- To create a model that allows the verification of student knowledge and their identification, as a source of information to attract talent for companies.
- To create a model that allows the construction of formal and non-formal education to adapt it to business reality, where a prototype of professional profiles is created, which includes more technical skills and representativeness of professional roles.
- To implement the "Proof of Stake" consensus algorithm in the system and compare the results with the already implemented in the system "Proof of Word" to study which of the two gives better results.

References

1. FlipowSki A (2018) Blockchain for 2018 and beyond: a (growing) list of blockchain use cases, 2018. [En línea]. https://medium.com/fluree/blockchain-for-2018-and-beyond-a-growing-list-of-blockchain-use-cases-37db7c19fb99.
2. Nakamoto S (2019) A peer-to-peer electronic cash system, Manubot, 11 2019. [En línea]. https://git.dhimmel.com/bitcoin-white paper/. [Último acceso: 24 04 2021]
3. Malviya H (2016) How Blockchain will defend IOT, SSRN 2883711
4. Wright A, De Filippi P (2015) Decentralized Blockchain technology and the rise of lex cryptographia, SSRN 2580664
5. Gräther W, Kolvenbach S, Ruland R, Ruland J, Torres C, Wendland F (2018) Blockchain for education: lifelong learning passport. In Proceedings of 1st ERCIM Blockchain workshop. European Society for Socially Embedded Technologies (EUSSET)
6. Atzori M (2017) Blockchain-based architectures for the internet of things: a survey, SSRN 2846810
7. Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, Yellick J (2018) Hyperledger fabric: a distributed

8. Maestre R (2019) La blockchain revolucionara la comunicacio de l'empresa, Comunicació: revista de recerca i d'anàlisi, pp 95–116
9. Mougayar W (2016) The business Blockchain: promise, practice and application of the next internet technology. Wiley, New Jersey
10. Marco I, Lakhani KR (2017) The truth about Blockchain. Harvard Bus Rev 95(1):118–127
11. Matilla J, Seppälä T (2015) Lockchains as a path to a network of systems. In An emerging new trend of the digital platforms in industry and society. ETLA-The Research Institute of the Finnish Economy
12. Garba A, Chen Z, Guan Z, Srivastava G (2021) LightLedger: a novel blockchain-based domain certificate authentication and validation scheme. IEEE Trans Netw Sci Eng 8(1):1698–1710
13. Yu K, Tan L, Shang X, Huang J, Srivastava G, Chatterjee P (2020) Efficient and privacy-preserving medical research support platform against COVID-19: a blockchain-based approach. IEEE Consum Electron Magazine 10(2):111–120
14. Atienza D (2018) Gestion de certificados academicos sobre la blockchain Ethereum, 06 09 2018. [En línea]. https://blogs.uoc.edu/informatica/gestion-de-certificados-academicos-sobre-la-blockchain-ethereum/. [Último acceso: 24 04 2024]
15. Gonzalez R, Paniagua F, Nombela JJ, Delgado C, Rodriguez C, Gil R, Sanjuan O, Chaveli E. CertiBlock: Emision y validacion de titulos universitarios con Blockchain, de In Congreso Internacional de Educacion Superior de Calidad en el Espacio Latinoamericano (ESCEL)
16. Gräther W, Kolvenbach S, Ruland R, Schütte J, Torres C, Wendland F (2018) Blockchain for education: lifelong learning passport. In: Proceedings of 1st ERCIM Blockchain workshop. European Society for Socially Embedded Technologies (EUSSET)
17. Juričić V, Radošević M, Fuzul E (2019) Creating student's profile using blockchain technology. In 2019 42nd international convention on information and communication technology, Electronics and Microelectronics (MIPRO) IEEE, pp 521–525
18. Nikolskaia K, Snegireva D, Minbaleev A (2019) Development of the application for diploma authenticity using the Blockchain technology. In International conference "quality management, transport and information security, information technologies (IT&QM&IS) IEEE, pp 558–563
19. Capece G, Levialdi Ghiron N, Pasquale F (2020) Blockchain technology: redefining trust for digital certificates. Sustainability 12(21):8952
20. Kanan T, Obaidat A, Al-Lahham M (2019) SmartCert blockchain imperative for educational certificates. In: 2019 IEEE Jordan international joint conference on electrical engineering and information technology (JEEIT), pp 629–633
21. Grupo de Trabajo Intersectorial de Crue Universidades Españolas, Informe de procedimientos de evaluación no presencial CRUE, 16 4 2016. [En línea]. Available: https://tic.crue.org/wp-content/uploads/2020/05/Informe-procedimientos-evaluaci%C3%B3n-no-presencial-CRUE-16-04-2020.pdf. [Último acceso: 24 4 2022].
22. SmartDegrees, SmartDegrees and TechHeroX certify corporate training with blockchain, 2019. [En línea]. https://www.smartdegrees.es/en/smartdegrees-and-techherox-certify-corporate-training-with-blockchain/. [Último acceso: 24 04 2022].
23. Ibermatica, Nace la primera aplicación de blockchain para la gestión interuniversitaria de títulos académicos, 29 1 2019. [En línea]. https://ibermatica.com/nace-la-primera-aplicacion-de-blockchain-para-la-gestion-interuniversitaria-de-titulos-academicos/. [Último acceso: 24 04 2022].
24. Turkanović M, Hölbl M, Košič K, Heričko M (2018) Kamišalić A (2018) EduCTX: a blockchain-based higher education credit platform. IEEE Access 6:5112–5127

25. Saleh OS, Ghazali O, Rana ME (2020) Blockchain based framework for educational certificates verification. J Critic Rev 7(03):79–84

26. Boeser B (2017) BMeet TrueRec by SAP: Trusted Digital Credentials Powered by Blockchain, 24 07 2017. [En línea]. Available: https://news.sap.com/2017/07/meet-truerec-by-sap-trusted-digital-credentials-powered-by-blockchain/. [Último acceso: 2022 05 09]

27. Khovratovich D, Law J (2017) Sovrin: digital identities in the blockchain era. Github Commit Jasonalaw 17:38–99

28. Cheng JC, Lee NY, Chi C, Chen YH (2018) Blockchain and smart contract for digital certificate I. In: EEE international conference on applied system invention (ICASI), pp 1046–1051

29. Gresch J, Rodrigues B, Scheid E, Kanhere SS, Stiller B (2018) The proposal of a Blockchain-based architecture for transparent certificate handling. In: International conference on business information systems, pp 185–196

30. Grech A, Camilleri AF (2017) Blockchain in education. Luxembourg: Publications Office of the European Union

31. Efanov D, Roschin P (2018) The all-pervasiveness of the blockchain technology. Procedia Computer Science 123:116–121

32. Legerén-Molina A (2019) Retos jurídicos que plantea la tecnología de la cadena de bloques, (Aspectos legales de blockchain)/Legal challenges about blockchain. Revista de Derecho Civil 6(1):177–237