Advances in Science, Technology and Engineering Systems Journal
Vol. 5, No. 6, 871-882 (2020)
www.astesj.com
Special Issue on Multidisciplinary Innovation in Engineering Science & Technology

ASTES Journal
ISSN: 2415-6698

Blockchain Application in Higher Education Diploma Management and Results Analysis

Fernando Richter Vidal*, Feliz Gouveia, Christophe Soares

Faculty of Science and Technology, University Fernando Pessoa, Porto, 4200-029, Portugal

ARTICLE INFO

Article history:
Received: 28 August, 2020
Accepted: 14 November, 2020
Online: 08 December, 2020

Keywords:
Blockchain
Blockchain Revocation
Higher Education
Digital Diplomas
Academic records
Blockcerts
Electronic document

ABSTRACT

Academic certifications are achievements desired by people, because they have a direct impact, positively, on their social lives. Such an important document, still widely issued in paper format, may be subject to forgery or impossibility of verification due to the unavailability of the issuing entity. This work consists of identifying, analyzing and testing some of the blockchain-based tools that are emerging, to offer more efficiency, reliability and independent degrees. A concept proof is presented, through the implementation of a prototype capable of issuing, verifying and sharing certificates. The results of this experiment are presented, analyzing the use of blockchain technology for this purpose. Finally, the work presents an overview of the current state of development and maturity in which these tools are found, reporting the advances and limitations, and exposing issues that still need to be resolved.

1 Introduction

This work is an extension of the work originally presented in 2019 at the international conference ”Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)” [1], which aims to present an analysis of the use of blockchain technology in the education area, for issuing and verifying academic degrees in higher education.

Academic certificates attest to the certificate holder’s abilities and skills and are accepted internationally [2]. These qualifications have a major impact on income and social position, both in emerging countries and in developed countries.

For example, in Brazil, data from *Pesquisa Nacional por Amostra de Domicilios Continuas* (PNADC) showed that the level of education is decisive for the Brazilian’s income [3]. According to the results presented, those who complete higher education achieve almost triple the remuneration compared to those who only have a high school education.

In Europe, according to Eurostat [1], every year higher education graduates in Europe exceed 4.5 million, in which France and the United Kingdom are the leading countries with over 740,000 graduates per year. The fraction of people with university degrees between 30 and 34 years old almost doubled in fourteen years, going from 23 % in 2002, to 39 % in 2016 [4].

As professionals become qualified, knowledge is directly transformed into income, and consequently in a better quality of life. Furthermore, these numbers confirm a continuous increase and constitute a solid basis that justifies the creation of solutions to verify the authenticity of university degrees.

The weakness of the paper model, which is still widely used, was even more evident during the crisis caused by COVID-19, in which the use of digital resources became indispensable.

Although digital initiatives have emerged to address these weaknesses [5], these solutions still depend on the issuing entity, concerning authenticity verification. Fortunately, blockchain promises to offer, besides this innovation, other improvements not yet achieved by digital solutions. Using the resources that the technology offers, it is possible to make the check process disconnected from the issuer and still guarantee authenticity.

The second innovation is related to privacy. Certificates are documents that contain personal information and are sensitive to data leakage. If, on the one hand, student privacy needs to be preserved, on the other hand, its distribution benefits those interested [6].

*Fernando Richter Vidal, Sao Joao da Boa Vista-SP Brazil,37705@ufp.edu.pt

[1] `http://ec.europa.eu/eurostat`

https://dx.doi.org/10.25046/aj0506104

Finally, blockchain solutions offer the third innovation compared to digital certificates, about timestamp. Due to the information being immutable and stored chronologically within the network, they accurately express the dates on which the events occurred.

This paper discusses the use of blockchain technology, aiming to benefit academic certificates with these possible innovations. The document is organized as follows: the next section provides a brief overview of blockchain technology; next, we describe the main differences between the blockchain solution and digital certificates; right after, we present the CertEdu prototype developed by *University Fernando Pessoa* (UFP), as well as a brief discussion of the results obtained and we conclude with some final remarks.

2 Background

2.1 *Blockchain*

Blockchain is a distributed system, formed by records that are organized in blocks and are linked to each other through cryptographic mechanisms. The technology became well known through the cryptocurrency Bitcoin [7], and soon expanded to several other applications.

There are three types of blockchain: public, private or consortium [8]. Public networks, also called permissionless blockchains, provides a free access environment to any participant who wants to join the network, however, the transaction validation rules are predefined and cannot be changed by any member. Typically, this type of blockchain implements the *Proof of Work* (PoW) consensus mechanism. In private networks, also called permissioned blockchain, the rules are defined according to the business interest. The organization that controls the network can define, for example, which users will decide on consensus or how to manage the network to accept new members. Finally, the consortium network is a category that merges properties from the public and private networks in the same environment. For example, in some scenarios, it would be interesting to keep the access public to the network, but also allow to make some data encrypted to preserve privacy and the anonymity of a participant.

Due to the consensus mechanisms and their *Peer-to-Peer* (P2P) topology, the network has gained strong protection against tampering. The success of an attempt of violation is conditioned to changes in all other previous blocks. Besides, attacks that would be able to take control of the network, such as a 51 % attack, would be extremely costly and could cost USD 500K per hour of processing [9]. In this aspect, the bigger the network, the more secure it becomes, which explains why Bitcoin is more secure when compared to other smaller networks [10]. This blockchain features results in an important property, which is immutability.

A block is always connected to a previous block, except for the genesis block, forming, then, a sequential chronological chain. The maximum size that a block can reach, depends on how each blockchain platform implements it. On Bitcoin, this value cannot exceed 1 Mb [11], while, on Ethereum there is no fixed limit, and the size change according to the number of gas units that can be spent per block (block gas limit).

As shown in figure 1, the block is organized in two areas: header and content. The header stores eighty bytes of control information. We find information like the hash header and the previous block; a software version, the target of the difficulty, a nonce, the root of Merkle [12], and a timestamp. Regarding the content area, they are stored as records. On average, a content area can store over five hundred transactions [5].

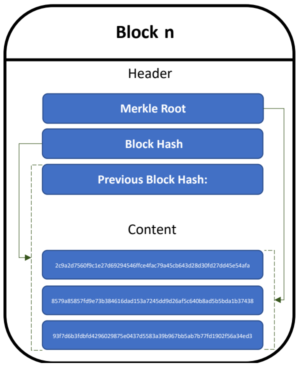

Block n
Header
Merkle Root
Block Hash
Previous Block Hash:
Content
2c9a2d7560f9c1e27d69294546ffce4fac79a45cb643d28d30fd27dd45e54afa
8579a85857fd9e73b384616dad153a7245dd9d26af5c640b8ad5b5bda1b37438
93f7d6b3fdbfd4296029875e0437d5583a39b967bb5ab7b77fd1902f56a34ed3

Figure 1: Overview of a Block Structure

Transactions are used to transfer an asset from one account to another account. The owner of an asset can move it inside the blockchain, through an account identified by a public address, which is controlled by its corresponding private key [13].

There is a conceptual difference between the public key and public address. The public key is used to verify the signatures generated by the private key's owner, while the address serves to identify the account. Using the example of Bitcoin, the process of generating the address is as follows: the public key is obtained by applying the function *Elliptic Curve Digital Signature Algorithm* (ECDSA) over the private key; the public key is subjected to two functions, *Secure Hash Algorithm* (SHA)-256, and *Race Integrity Primitives Evaluation Message Digest* (RIPEMD)-160; the resulting string size is reduced by passing the function *Base58Chech*, resulting in an address like $mgAzKQZZi47g4UMvmGJCsicbJ4P3B8SHRr$ [14].

In the next sections, will be discussed how academic certificates can be used as assets in the blockchain. Through the CertEdu application implemented by UFP, questions such as authenticity will be analyzed, as well as universities and students can have their identities verified. Finally, the results obtained by systematic tests are analyzed.

2.2 *Certification*

Certification involves three processes: issuing, verification, and sharing [15]. This paper evaluates the application of blockchain in each one of the processes, mainly in the verification and sharing. The digital certificates innovate compared to the paper model but do not guarantee verification and sharing because they depend on central points. As Schär notes, academic certificates are useful, only if they can be verified [6].

The disruptive technology of the blockchain allows creating a structure capable of making the verification process independent [16]. The figure 2 presents a typical scenario, in which the university, the student, and the employer are involved. Note that Jane's certificates can be verified directly on the blockchain, without contacting the university.

Table 1: Comparative between digital certificates vs. blockchain solutions

Properties	**Digital Certificate**	**Blockchain Certificate**
Reliability	Relies only in the digital signature	Several cryptography mechanisms are used
Privacy	All information are available in the certificate	Only the hash is public
Autonomy	Depend on central regulatory bodies	Technology eliminates the need for third parties
Data Loss	Depend on backup mechanisms	Standard normal distribution
Proof of existence	Dates relies on the suitability of the subscriber	Timestamp represent the date of the facts

Table 2: Comparison between the tools analyzed

Criteria	BTCert	Hyperledger	EduCTX	Blockcerts
Blockchain agnostic	no	no	no	yes
Self-sovereign identity	yes	yes [2]	yes	yes
Community with active user	no	yes	no	yes
Public network	yes	no	no	yes
Privacy concerns	yes	yes	yes	yes

The public information available on the blockchain says nothing about the student. This occurs thanks to the use of the hash, which records the certificate in a unidirectional way on the network, not allowing to retrieve any personal information from Jane. As a result, Jane has the autonomy to share the digital certificate file, only with whomever she wants, and everyone who receives the file will also be able to check it independently on the blockchain.

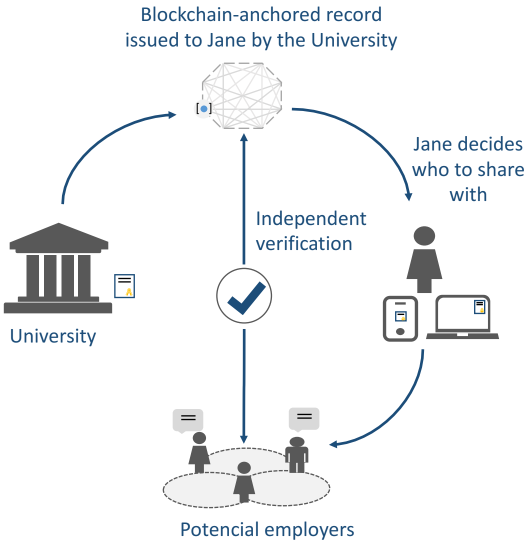

Blockchain-anchored record
issued to Jane by the University
Jane decides who to share with
Independent verification
University
Potencial employers

Figure 2: Diploma verification [1]

The table 1 presents a comparison between the properties of the digital certificate solution and the blockchain certificate solution. The blockchain innovation is realized in several aspects. The technology is more secure because unlike the digital certificate, in which all security depends relies only on the digital signature, the use of different cryptographic mechanisms, combined with the adoption of a distributed ledger, offers certificates a higher level of security.

Regarding privacy [17], digital certificates are much more sensitive to data leakage, considering that all personal information is contained in the certificate. This fact can restrict its replication. Analyzing this property in the blockchain solution, the distributed information says nothing about the student, and the certificate can be published without worries.

Digital signatures depend on central regulatory bodies. In some countries, there is not even an authority capable of certifying a signature [15]. In this aspect, blockchain offers complete autonomy, eliminating the need for third parties.

The blockchain, mainly in public architectures and consortium [8], offers a genuine backup mechanism since all information is replicated in pairs. Digital certificates, on the other hand, are easy to destroy electronically and depend on sophisticated backup mechanisms to avoid disappearing [15].

Finally, about the proof of existence, the reliability of the dates generated by digital certificates relies on the reliability of the subscriber. This can be a problem when a university has its private key stolen, and an attacker uses it to sign valid certificates with dates retroactive to the reported date of the theft. In this regard, the blockchain allows identifying the timestamp. As Ronning says, ”every credential issued with a stolen key must fail” [18].

3 CertEdu

3.1 Frameworks analyzed

The CertEdu project begins with the choice of the tool which will be used in the development. In 2018, when the project started, there were not many tools available for this purpose. The use of blockchain in the issue of academic certificate management is re-

[2] Shout combine Hyperledger Fabric + Hyperledger Indy

cent and the first students to receive their diplomas anchored in the blockchain, were from *Massachusetts Institute of Technology* (MIT), in 2017 [19].

We identified four potential platforms. The table 2 shows the comparison between them, and the used evaluated criteria.

Between the evaluated solutions, the Blockcerts tool was chosen to implement the prototype of this paper. The reason was that it better serves the requirements placed, especially about working on any blockchain. In reality, Blockcerts was the only certificate issuing solution that was born with the requirement to work for any blockchain. This requirement greatly increases the complexity of the solution, but it is important because it keeps the application life cycle long. Another point that drew attention is its active community of developers, which makes the project receive constant updates.

Interesting points were also noted on other platforms.

BTCerts, a project inspired by the MIT solution, address to the problem of centralizing the revocation process of Blockcerts. The model proposed by BTCerts solves the issue and can be easily adapted to any type of blockchain, but the costs are concernedly, mainly because it does not explain how the complementary revocation information would be registered, since the OP_RETURN_DATA field has a limited size of 83 bytes [20].

EduCTX, although having a more focused approach to digitizing credits *European Credit Transfer and Accumulation System* (ECTS), the solution brings an approach about how to use the multiple signatures, involving the student and institution to validate the transaction. The solution also raises an interesting question regarding the consensus mechanism used. Depending on the type of application, one consensus mechanism is more suitable than another. Considering education, it makes no sense to mine blocks to record transactions that contain academic certificates or ECTS credits. Universities are reliable nodes and responsible for the data they provide. Operating in a permissive way to create transactions, universities maintain autonomy in the issuing process, but they are unrelated about verification and sharing.

On Hyperledger's evaluation, its flexibility was identified as a strong point, and as a weak point, the lack of models capable of speeding up development. It would be interesting if pre-assembled open-source libraries existed for that purpose. Another issue involving Hyperledger is that to identify the university or the student, it would be necessary to combine the use of two greenhouse technologies (Fabric + Indy), which can make the development of the application even more complex.

Recently, the use of smart contracts has been evaluated for academic record systems[13, 21, 22, 6, 23, 24]. Prototypes are implementing this type of mechanism in the Blockcerts [3], but they are new and still being discussed. This type of approach is interesting but needs to be observed, because not every blockchain implements this type of contracts (example Bitcoin). Besides, the languages implemented by different blockchains can be different, which can make it difficult to create a standard. In the examples shown, the vast majority are based on Ethereum. We believe that because blockchain technology is recent, with many networks likely to disappear and others appearing in the future, the proposed solution should be compatible with any blockchain technology [5] [1]. Also, the blockchain scalability issue [25], may encourage applications to migrate to smaller networks.

3.2 Prototype

UFP has built a prototype and has been testing the application of academic certificates with blockchain technology. The application called CertEdu was built based on the Blockcerts platform and has its architecture designed according to the figure 5. As you can see, CertEdu issues electronic documents on Bitcoin and Ethereum networks. The objective of implementing two networks is precisely to assess the prototype's ability to achieve the desired blockchain compatibility property.

The implementation described in this work shows that even existing different ways to operate the blockchains (permissioned, permissionless, consortium), the implemented solution is easily adapted to operate on any type of network because of these reasons:

- The solution uses its own Merkle Proofs mechanism
- The technique of anchoring the diploma hash on the blockchain, allows verification and overcomes the space limitation
- The solution doesn't need the use of smart contracts

The technical standard of Blockcerts was designed to work with any blockchain, thus preventing the success of the project from being conditioned to the evolution of another product. In 2017 when the project was started, integration was only possible with Bitcoin, but it soon extended to Ethereum. In 2018, Universidad del Rosario, in Colombia, [26] built the integration with Hyperledger.

Blockcerts uses different layers that work together to create the hashes for each batch of certificates, issuing them on the blockchain and subsequently allowing web platforms to print the certificates by using *JavaScript Object Notation* (JSON) objects and verifying them on the blockchain [4].

The figure 3 shows a process of creating a digital certificate on the blockchain by using the components of Blockcerts. As we can see, the asset stored is the hash of the JSON generated file, which in practice means linking the digital file with the blockchain.

The next section describes CertEdu implementation.

3.2.1 Certificate templates

Cert-tools is responsible for creating the certificate templates that will later be signed and anchored on the blockchain. For each model, it is possible to customize information such as the title, logo, description, history. There are also customizable fields, so that peculiar information can be treated. These fields can be created globally (they will appear for all the certificates generated from the model in question) or by the recipient (they will only appear for a specific group of recipients). Next, part of the code of interaction with the component is presented.

[3] https://community.blockcerts.org/t/introducing-smart-contracts-to-blockcerts/2362

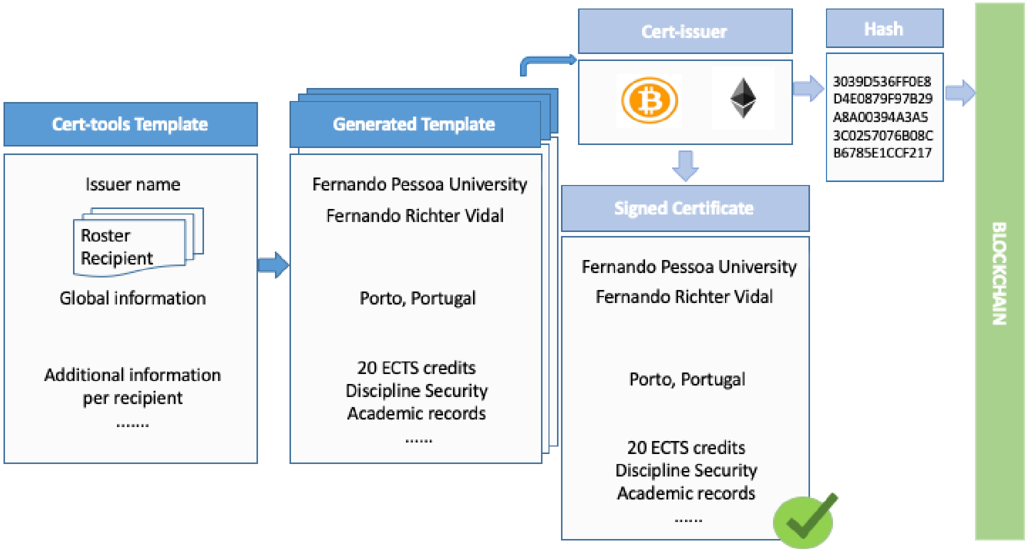
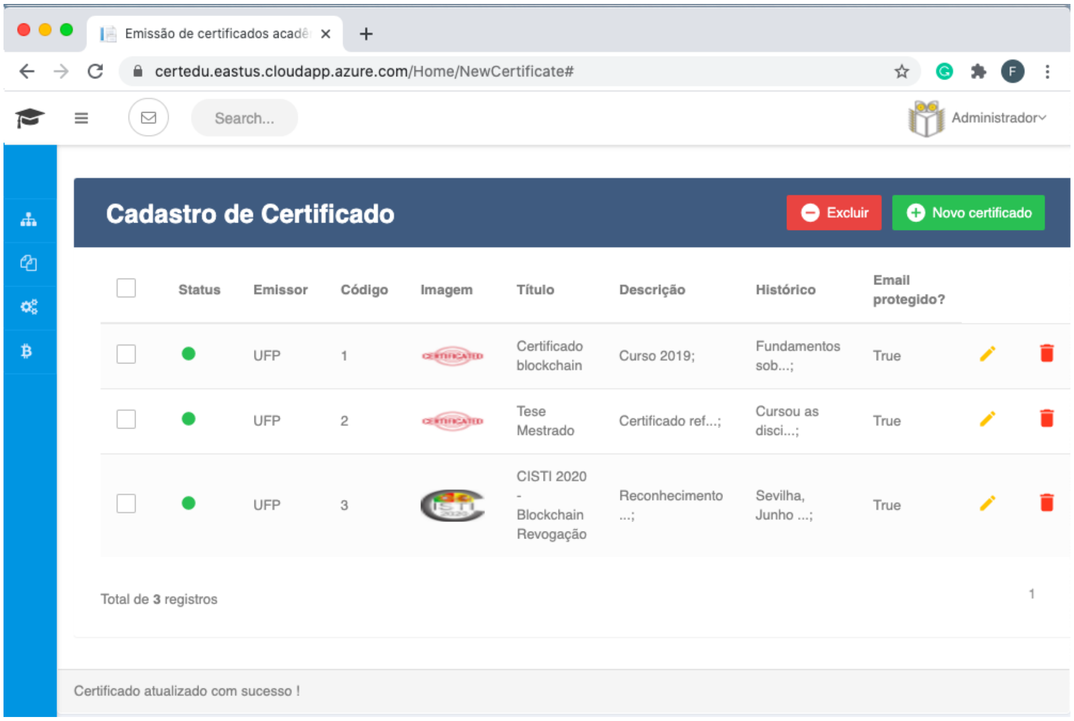


Figure 3: Diploma configuration [1]


Emissão de certificados acadê
certedu.eastus.cloudapp.azure.com/Home/NewCertificate#
Search...
Administrador
Excluir
Novo certificado

Cadastro de Certificado

☐	Status	Emissor	Código	Imagem	Título	Descrição	Histórico	Email protegido?		
☐	●	UFP	1	CERTIFICATED	Certificado blockchain	Curso 2019;	Fundamentos sob...;	True	✎	🗑
☐	●	UFP	2	CERTIFICATED	Tese Mestrado	Certificado ref...;	Cursou as disci...;	True	✎	🗑
☐	●	UFP	3	ISTI 2020	CISTI 2020 - Blockchain Revogação	Reconhecimento ...;	Sevilha, Junho ...;	True	✎	🗑

Total de 3 registros

1

Certificado atualizado com sucesso !

Figure 4: CertEdu's Certificate Template

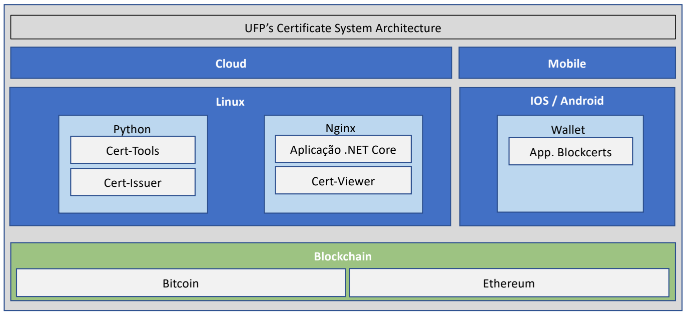


Figure 5: UFP Architecture [1]

```
create-certificate-template -c /ufp/model/ConfigJson_UFP.ini
--data_dir /ufp/ --template_dir /ufp/model
--template_file_name /ufp/model/UFP_3.json
--issuer_logo_file /ufp/image/UFP.png
--cert_image_file /ufp/image/UFP_3.png
--issuer_url https://certedu.eastus.cloudapp.azure.com/
--issuer_email ufp@ufp.edu.pt
--issuer_name 'Universidade Fernando Pessoa'
--issuer_id https://certedu.eastus.cloudapp.azure.com/UFP_1.json
--revocation_list
 https://certedu.eastus.cloudapp.azure.com/rev_UFP_1.json
--issuer_certs_url https://certedu.eastus.cloudapp.azure.com
--certificate_description 'Reconhecimento de apresentação no congresso.'
--certificate_title 'CISTI 2020  - Blockchain Revogação'
--criteria_narrative 'Sevilha, Junho de 2020'
--issuer_public_key ecdsa-koblitz-pubkey:
```

```
mgAzKQZZi47g4UMvmGJCsicbJ4P3B8SHRr
--badge_id 370820c5-59ff-4a0b-8c9c-55faa0b9f431
--unsigned_certificates_dir /ufp/unsigned
```

Cert-tools receives as an input the information that will form the certificate and as output, returns a file JSON, ready to be signed by the next component. The file in question is generated by a Blockcerts module called cert-schema [4], which is based on the *Verifiable Credentials* (VC) [5]. The data types mapped by the standard follow the norm *Internationalized Resource Identifiers* (IRIs), the same used by XMLSchema [6]. All this concern in following these standards is to offer entities and interested parties a standardized format for certifications.

The figure 4 shows the implementation of cert-tools in CertEdu. The model stored in the database contains the necessary parameters for the issuance of a certificate. In another system interface, all it takes is to link the model code with a list of students in order to publish the certificates. Note that there is a status indicator, which checks when saving the record if all settings have been applied successfully. For example, there is a parameter that allows you to indicate the public address of the certificate. When it is activated, the application tries to publish on the indicated website with the parameterized access credentials. If it fails, the model remains pending and cannot be used until the error is fixed.

3.2.2 *Publishing area*

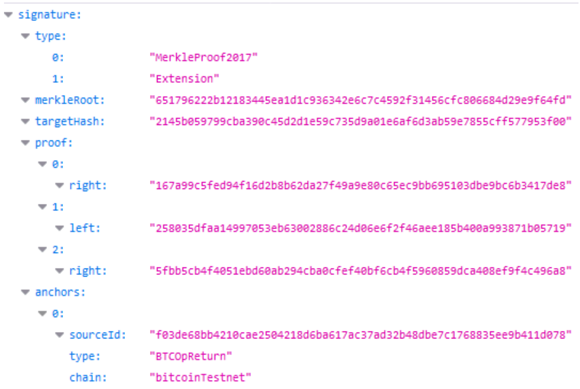
Cert-issuer is the component responsible for generating the transaction on the blockchain. The input receives the diploma file generated by cert-tools and returns as output the diploma hash published on the blockchain. Its role, in addition to the signing, is to allow blockchain compatibility, by providing a structure that allows connectors from other networks to be implemented. In the component area called blockchain_handlers, all it takes it to create three functions to connect a new network: connection (connectors.py), transaction (transaction_handlers.py), and subscriber (signer.py). On top of that, it is necessary to change the block below the main function of the component.

```
issue_certificate.py

def main(app_config):
    chain = app_config.chain
    if chain == Chain.ethereum:
        from cert_issuer.blockchain_handlers import ethereum
        certificate_batch_handler, transaction_handler,
        connector = ethereum.instantiate_blockchain_handlers(app_config)
    elif chain == Chain.bitcoin:
        from cert_issuer.blockchain_handlers import bitcoin
        certificate_batch_handler, transaction_handler,
        connector = bitcoin.instantiate_blockchain_handlers(app_config)
    else:
      new blockchain
        ...

    return issue(app_config, certificate_batch_handler,
    transaction_handler)
```

The standard is maintained by the open-source community, to support networks the Bitcoin and Ethererum. The integration to other networks is emerging as initiatives do, such as the University of Rosario, in Colombia [26], which built the connector for Hyperledger, and is testing it experimentally.

Another notable point of the figure 3 is the possibility of signing a group of models at once. Technically, cert-tools generates several certificate files and calculates the group's Merkle root, recording this value on the blockchain.

The figure 6 shows the structure of a certificate file that makes up a batch. All files in the batch have the same value as the merkleRoot field, and additionally store, in addition to the hash itself, the hashes of the nodes needed to verify the root of Merkle (proof 0, 1 and 2 of 6). In practice, when the verifier receives a file, it calculates the hash and checks on the blockchain whether this file belongs to the generated batch. With that, you only need to spend a single time, to be possible to check *n* certificates. Also, this check is very useful for revocation, because canceling a single blockchain registration automatically cancels the entire batch.



```
signature:
  type:
    0:          "MerkleProof2017"
    1:          "Extension"
  merkleRoot:   "651796222b12183445ea1d1c936342e6c7c4592f31456cfc806684d29e9f64fd"
  targetHash:   "2145b059799cba390c45d2d1e59c735d9a01e6af6d3ab59e7855cff577953f00"
  proof:
    0:
      right:    "167a99c5fed94f16d2b8b62da27f49a9e80c65ec9bb695103dbe9bc6b3417de8"
    1:
      left:     "258035dfaa14997053eb63002886c24d06e6f2f46aee185b400a993871b05719"
    2:
      right:    "5fbb5cb4f4051ebd60ab294cba0cfef40bf6cb4f5960859dca408ef9f4c496a8"
  anchors:
    0:
      sourceId: "f03de68bb4210cae2504218d6ba617ac37ad32b48dbe7c1768835ee9b411d078"
      type:     "BTCOpReturn"
      chain:    "bitcoinTestnet"
```

Figure 6: Certificate batch structure

Blockcerts implements an independent version of the Merkle root, the 2017 Merkle Proof Signature Suite [7]. This means that the field calculated in the JSON file, always follows the same pattern, contributing at this point for the tool to work on several networks. Each blockchain can implement the field differently, as is in the case Ethereum, which unlike Bitcoin, uses Merkle Patricia [27].

3.2.3 *Embedded authenticity checker*

The verifier has two roles: to inform the authenticity of a certificate and to represent it graphically to the user. The first versions of this component in Blockcerts were called cert-viewer, but later changed to blockcerts-verifier [8].

The technology is based on JavaScript, which makes it easier for applications, such as CertEdu (Figure 8), to embark on a universal certificate verifier within its structure.

[4] https://github.com/blockchain-certificates/cert-schema

[5] https://www.w3.org/TR/vc-data-model/

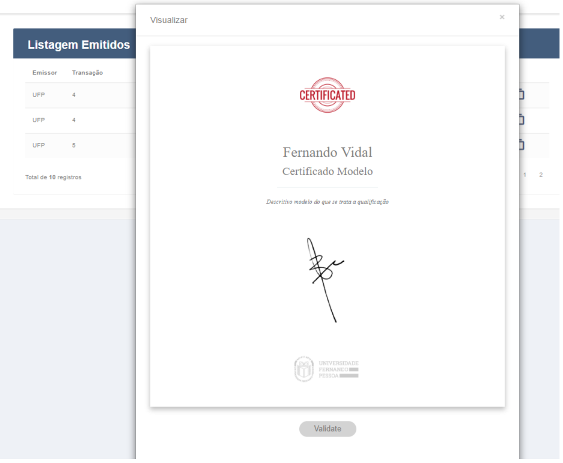
[6] http://www.w3.org/TR/xmlschema-2/

[7] https://w3c-dvcg.github.io/lds-merkleproof2017/

[8] https://github.com/blockchain-certificates/blockcerts-verifier

How the issuance process is implemented, directly impacts on the complexity of implementing this component. Notably, Blockcerts seeks to use standardized components of the blockchain, such as hashes, transaction recording, Merkle root. With this, the inclusion of new blockchain in the operation of the blockcerts-verifier becomes a simpler process. Considering a different scenario, in which the mechanisms use smart contracts, depending on the way it is implemented, this process of incorporating new networks can become complex.

There is still no defined standard on the display format of the digital certificate (figure 7 and 8). Although this is not a technical security problem, it can cause some distrust for an appraiser who receives the same diploma issued by the same broadcaster but in different formats. Fortunately, the verification function can guarantee the data veracity to the interested party, and can even validate the file in different universal verifiers, such as the one offered by Blockcerts [9]


Listagem Emitidos

Emissor	Transação
UFP	4
UFP	4
UFP	5

Total de 10 registros

Visualizar

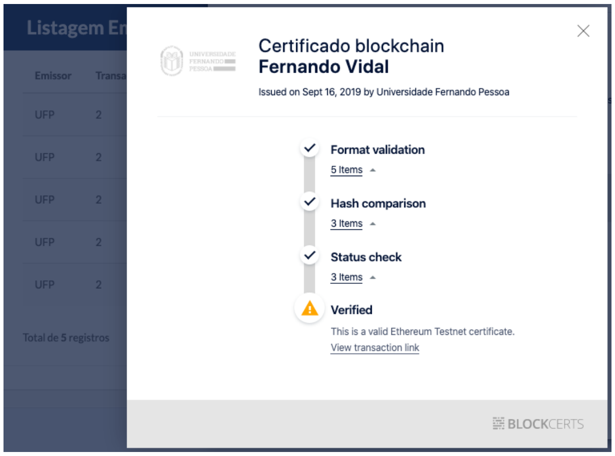
CERTIFICATED

Fernando Vidal
Certificado Modelo

Descritivo modelo do que se trata a qualificação

UNIVERSIDADE FERNANDO PESSOA

Figure 7: Model 1 for viewing a digital certificate issued by Blockcerts


Listagem Em

Emissor	Transa
UFP	2
UFP	2
UFP	2
UFP	2
UFP	2

Total de 5 registros

UNIVERSIDADE FERNANDO PESSOA

Certificado blockchain
Fernando Vidal
Issued on Sept 16, 2019 by Universidade Fernando Pessoa

✓ **Format validation**
5 Items

✓ **Hash comparison**
3 Items

✓ **Status check**
3 Items

⚠ **Verified**
This is a valid Ethereum Testnet certificate.
View transaction link

Figure 8: Model 2 for viewing a digital certificate issued by Blockcerts

3.2.4 Mobile application

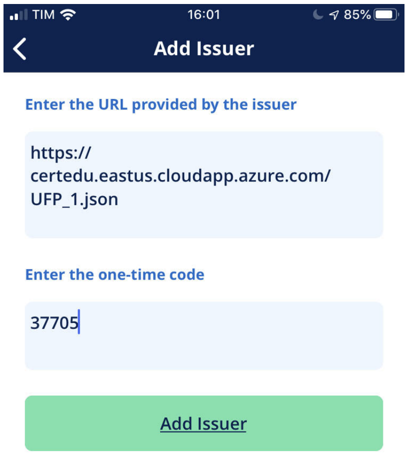
Cert-wallet is a Blockcerts application, also available in an open-source format, which aims to offer users autonomy over their records. Once the user downloads the application on their device, their identity is linked to a phrase created automatically by Blockcerts, which becomes a kind of private key.

The student is sovereign to register an issuer in his account and redeem the certificates that were issued by him. Autonomy is also evidenced by the fact that the student has the freedom to send his diploma to whomever he wishes, directly, without the intervention of any third parties. The difference between the digital process and the paper is that the registration received by the third party can be verified directly on a public blockchain network (in the case of this paper, Bitcoin or Ethereum), without any consultation with the issuing university.

The application has three main functions:

1. Automatically generate and send the student's public address to the sending systems
2. Store the digital certificates
3. Share the digital certificates

The figure 9 shows the operation of the first function of the cert-wallet. Note that the user informs an address of a sender profile file, and also a unique and disposable code, in English, called the nonce. This code serves as a kind of student credential to access the available service. Right after this procedure, cert-wallet accesses another address that is embedded in the profile file, and sends it to that address, the public key generated by the application, and also the code entered.



Add Issuer

Enter the URL provided by the issuer

https://certedu.eastus.cloudapp.azure.com/UFP_1.json

Enter the one-time code

37705

Figure 9: Cert-wallet application interface responsible for generating the student's public address

On the other side of the operation, in the second address mentioned software that is prepared to receive the public key and compare the received code is operating, validating, or not the message. If so, the cert-wallet receives a signal to register the issuer in its

[9] https://www.Blockcerts.org/

database, and the student's public address is stored in the issuing application so that it can be used in future issues.

The second function of the application refers to the storage of certificates, which, as noted in the figure 10, can be done in two ways: informing an address *Uniform Resource Locator* (URL) in which the certificate is published, for example, `https://certedu.eastus.cloudapp.azure.com/certdata/2137705.json`, or by directly importing a JSON file.

Immediately after importing a credential, the application starts a process of validating and verifying the authenticity of the file, informing at the end of the process whether the certificate is valid or not.

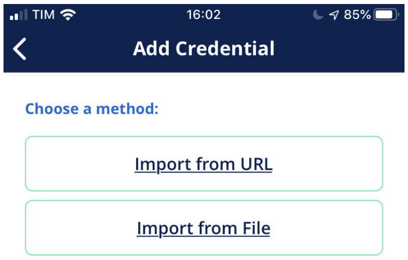


Figure 10: Ways to store a certificate in the cert-wallet

The third and final function of the cert-wallet, refers to the possibility given to the users to share their certificates. When selecting a certificate, it is possible to physically send the file to another user or simply provide the address that references it.

Table 3: Processes and challenges related to the blockchain solution

Process(s)	Challenge	Satisfies
Issuing	A feasible financial solution to large issuing	Yes
Issuing	Identify of universities	Yes
Issuing	Allow revocation	Partial
Verifying	Verifying em local database (decentralizing)	Partial
Verifying	Verifying in universal verifier	Yes
Verifying	High availability	Yes
Sharing	Identify of students	Yes
Sharing	Sovereign to share the certificates	Yes
Sharing	Graphical display of recorded information	Yes
All	Operating compatibility on any type of blockchain	Yes

3.2.5 Goals

The purpose of the application is to simulate an environment close to a real situation, for this reason, it was decided to configure the TestNet (Bitcoin) and Rospten (Ethereum) networks. Faucets [10], [11], [12], [13] were used to transfer credits to the application's accounts, and thus emulate a scenario close to reality, in which there are limited financial resources to generate certificates.

The table 3, presents an analysis by the process, about the main challenges to be addressed. In this way, the work assesses such issues through CertEdu, and highlights which issues are addressed and which still need to be addressed. Concerning the points not yet solved, some possible solutions to these problems are presented.

Below, the topics partially covered are discussed.

3.2.6 Disconnected checking and revocation

One of the innovations proposed by blockchain certificate solutions is disconnected verification. For example, it would be possible to verify the authenticity of the diplomas, using an off-line local copy. All certificates that are already there are perfectly verifiable.

However, the prototype found that this feature was not met, due to the way Blockcerts implements the verification process. There is a dependency on two external files (hosted on the issuer's server), one for university identification, and another for checking certificate revocation.

Regarding the first dependency, Learning Machine and NextID in late 2019, published an article [18] with a proposal to replace the issuer profile. This functionality must be present in versions 3.0 of blockcerts.

Regarding revocation, there is still no definitive solution to the problem. The paper [5], presents different approaches, such as smart contracts [28], control data [29] or even the combined use of *Interplanetary File System* (IPFS) and blockchain [30] , [31], [32].

3.3 Systemic tests

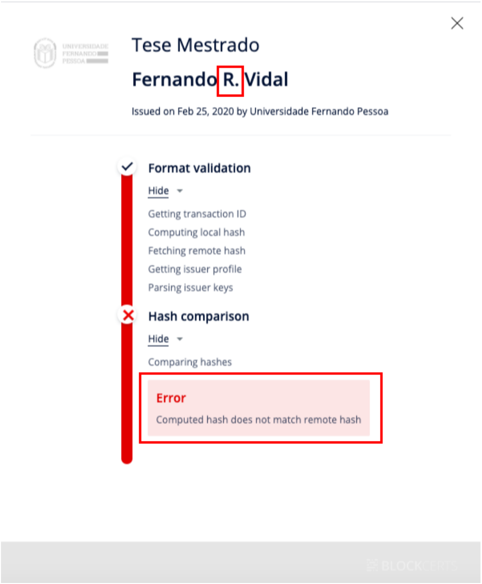
The following tests simulate some of the situations that can occur when issuing a blockchain certificate. Firstly, attempts are made to tamper the certificate, either through data editing or through the usurpation of property. Right after this test, it is evaluated how the validation system behaves in a disconnected way.

3.3.1 Tamper

In this simulation, a diploma issued by CertEdu is changed. Using a simple text editor, the original information of the diploma is modified, including a letter R in the student's name. It is notable that the digital diploma file is not encrypted, and can be easily edited by users who have a minimum of knowledge in text editing tools.

The result of the modified document validation operation can be seen on the figure 11, and the rules processed by the verifier can be observed through the table 4.

[10] `https://faucet.ropsten.be/`
[11] `https://faucets.blockxlabs.com/ethereum`
[12] `https://coinfaucet.eu/en/btc-testnet/`
[13] `https://bitcoinfaucet.uo1.net/send.php`



Tese Mestrado

Fernando R. Vidal

Issued on Feb 25, 2020 by Universidade Fernando Pessoa

Format validation

Hide

Getting transaction ID

Computing local hash

Fetching remote hash

Getting issuer profile

Parsing issuer keys

Hash comparison

Hide

Comparing hashes

Error

Computed hash does not match remote hash

Figure 11: Tampered certificate validation

Table 4: Result of validations performed by the universal verifier

Nº	Rule	Satisfies ?
1	The transaction number contained in the certificate (sourceId) exists in the referenced blockchain ?	Yes
2	The computed hash over the information, match with the targetHash field?	Yes
3	The *targetHash* match with the blockchain stored content ?	No
4	The issuer's public address (server) is available ?	Yes
5	The embedded issuer's public key in the certificate, match with the key hosted in the issuer's server	Yes

We realized in this experience that the verifier can identify any adulterations of the file's content. Analyzing the verifier's rules, even if an attacker tampered a certificate and recalculated the hash data, the tamper would be detected, because the content of the *targetHash* field would not match the value stored in the blockchain.

3.3.2 Unauthorized appropriation

This other fraud simulation discusses the possibility for an attacker to change the issuers and /or recipients of a genuine certificate. For example, it would be interesting for criminals to replicate real university certificates with lesser visibility, changing them as if they were from prestigious universities. Likewise, a profitable fraud would be to offer genuine degrees to malicious recipients, who only intend to accumulate ”achievements”.

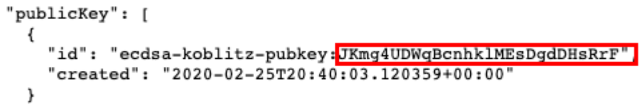
Blockcerts embed the student's public key in the certificate data, in the *recipientProfile* section, in the *publicKey* field. Likewise, in the *verification* section, the sender's information is embedded. This means that such fields are part of the hash calculation, which guarantees protection against tampering.

However, an attacker could alter the certificate data, informing other public keys of issuers and recipients, and recalculate the certificate hash. Additionally, to prevent rule 3 (table 4) from identifying the fraud, the attacker could change the *sourceId* field for a transaction that he created, which contains exactly the value of the hash of the defrauded certificate.

In this case, rule 3 will pass as true, because both the local calculation of the hash and the comparison with the information stored in the blockchain will be considered valid. However, Blockcerts can identify this fraud, because in addition to validating the content of the transaction, it checks whether the address of the transaction is owned by the issuing university. This is possible because the system compares the public address of the transaction with the public address hosted on the sender's server.

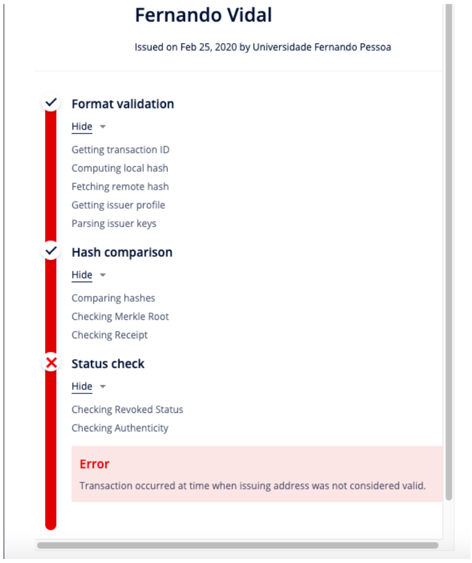
The figure 12 presents excerpts from the university's profile file, highlighting the public key information. The adulterated certificate, and the forged transaction, point to the $mgAzKQZZi47g4UMvmGJCsicbJ4P3B8SHRr$ hash. However, the university's real public key points to the value $JKmg4UDWqBcnhklMEsDgdDHsRrF$.

As shown in figure 13, the validator detects the inconsistency of this information, preventing the fraud from being carried out.



```
"publicKey": [
  {
    "id": "ecdsa-koblitz-pubkey:JKmg4UDWqBcnhklMEsDgdDHsRrF",
    "created": "2020-02-25T20:40:03.120359+00:00"
  }
```

Figure 12: Issuer identification file



Fernando Vidal

Issued on Feb 25, 2020 by Universidade Fernando Pessoa

Format validation

Hide

Getting transaction ID

Computing local hash

Fetching remote hash

Getting issuer profile

Parsing issuer keys

Hash comparison

Hide

Comparing hashes

Checking Merkle Root

Checking Receipt

Status check

Hide

Checking Revoked Status

Checking Authenticity

Error

Transaction occurred at time when issuing address was not considered valid.

Figure 13: Certificate check with the issuer tampered with

3.3.3 Stolen key and revocation

This simulation evaluates Blockcerts' ability to identify frauds that may occur in situations where the university has had its private key stolen.

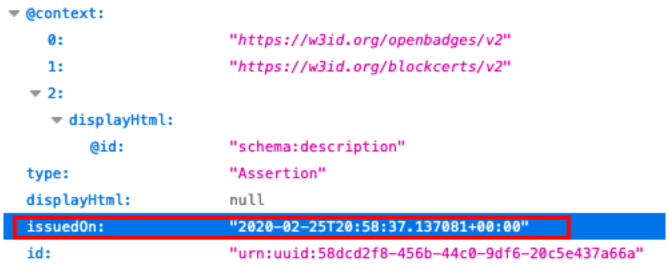
The digital diplomas issued by non-blockchain solutions, such as those that sign using a *Rivest-Shamir-Adleman* (RSA) key, do not guarantee in their signature proof that the creation date associated with their signature is consistent with reality. In most cases, the issuer who signs with the keys to their property, must sign with the correct date and time [18].

In situations where the private key is stolen, the attacker may want to issue retroactive diplomas, thus managing to guarantee illegal conquests for any recipient.

When the university realizes that its key was stolen, it revokes the validity from the date on which the theft occurred. However, in non-blockchain solutions, since certificate dates cannot be trusted, it is very difficult to determine which diplomas are still valid.

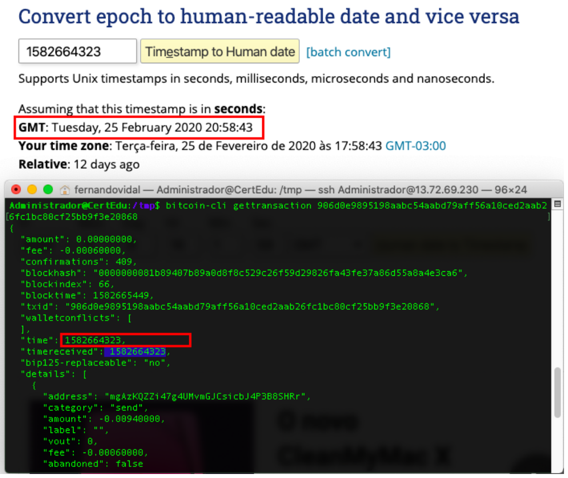
Therefore, by using a blockchain's reliable timestamp, you can calculate the actual date of issuance of a diploma, and thus, determine the revocation/expiration. With that being said, it becomes more reliable to separate valid and invalid credentials. For example, all credentials that are referenced on a blockchain, before the reported date of the theft, remain securely valid and are not affected by any revocation process.

The figures 14 and 15, demonstrate how the date of the issuance of a certificate can be easily compared with its registration on the blockchain. By consulting the date of the corresponding transaction (indicated in the *sourceId* field), you can easily perform the comparison.



```
▼ @context:
    0:                "https://w3id.org/openbadges/v2"
    1:                "https://w3id.org/blockcerts/v2"
  ▼ 2:
    ▼ displayHtml:
        @id:          "schema:description"
type:                 "Assertion"
displayHtml:          null
issuedOn:             "2020-02-25T20:58:37.137081+00:00"
id:                   "urn:uuid:58dcd2f8-456b-44c0-9df6-20c5e437a66a"
```

Figure 14: Certificate issue date



Convert epoch to human-readable date and vice versa

1582664323 | Timestamp to Human date | [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:
GMT: Tuesday, 25 February 2020 20:58:43
Your time zone: Terça-feira, 25 de Fevereiro de 2020 às 17:58:43 GMT-03:00
Relative: 12 days ago

fernandovidal — Administrador@CertEdu: /tmp — ssh Administrador@13.72.69.230 — 96×24

```
Administrador@CertEdu:/tmp$ bitcoin-cli gettransaction 906d0e9895198aabc54aabd79aff56a10ced2aab2
6fc1bc80cf25bb9f3e20868
{
  "amount": 0.00000000,
  "fee": -0.00060000,
  "confirmations": 409,
  "blockhash": "0000000081b89407b89a0d8f8c529c26f59d29826fa43fe37a86d55a8a4e3ca6",
  "blockindex": 66,
  "blocktime": 1582665449,
  "txid": "906d0e9895198aabc54aabd79aff56a10ced2aab26fc1bc80cf25bb9f3e20868",
  "walletconflicts": [
  ],
  "time": 1582664323,
  "timereceived": 1582664323,
  "bip125-replaceable": "no",
  "details": [
    {
      "address": "mgAzKQZZi47g4UMvmGJCsicbJ4P3B8SHRr",
      "category": "send",
      "amount": -0.00940000,
      "label": "",
      "vout": 0,
      "fee": -0.00060000,
      "abandoned": false
```

Figure 15: Registration date of certificate issuance on the blockchain

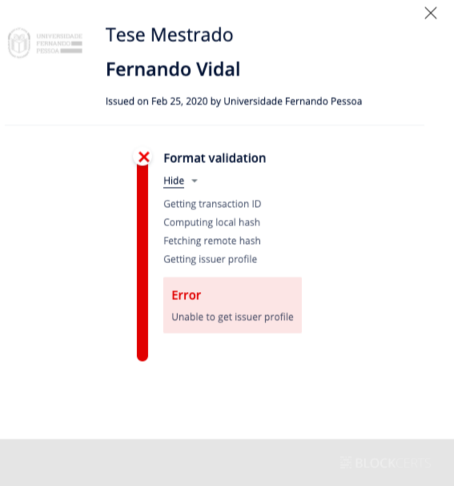
In this matter, it is concluded, that the blockchain solution offers a differential about the solutions without blockchain, since it guarantees students, that their old diplomas will not be affected, even if unexpected situations like a private key theft happens.

3.3.4 Validation without server access

This simulation is divided into two parts. First, the possibility of the issuer's server failing is evaluated and then the functionality of continuing to validate in a non-synchronized way, records on a local blockchain are tested.

In this first test, the sender's server is inaccessible. This simulation intends to evaluate the system's behavior when faced with a failure of the university server. For this, the server on which the profile and revocation files are hosted was turned off and was performed a check for a genuine certificate.

It can be seen through figure 16, that the verifier was unable to tell whether the certificate was valid or not.



Tese Mestrado

Fernando Vidal

Issued on Feb 25, 2020 by Universidade Fernando Pessoa

Format validation

Hide

Getting transaction ID
Computing local hash
Fetching remote hash
Getting issuer profile

Error
Unable to get issuer profile

Figure 16: Local check, error when connecting transmitter

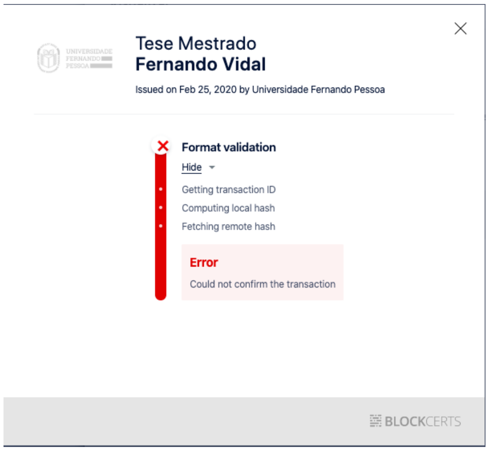
The test concludes that the solution is not yet capable of offering independence from the issuer. Besides, if an attacker manages to invade the server, even if it is temporarily, it would be possible to carry out the attacks described in the 3.3.1 section, due to the possibility of changing the information stored in the sender's profile.

In the second test considers a scenario in which the local blockchain is not synchronized. One of the benefits of using the blockchain would be the possibility to continue to validate certificates, on a local blockchain, even if it no longer exists.

Analyzing the libraries of the implemented prototype, it is noticed that the verifier uses interfaces *Application Programming Interface* (API), made available by block query tools, to verify them. This means that for a local validation it would be necessary to modify the verification address for the local base. As this is a relatively easy operation, it can be said that the tool meets this requirement.

Another situation that can be simulated is the verifier validating the issuance of a certificate that has not yet been authorized by the consensus mechanisms. As mentioned in the section, the validation of the blocks is one of the pillars that brings all the security of the technology. Validating a diploma from a registration that has not yet been confirmed could be considered a very serious failure.

Figure 17 shows the result of this operation, and as the result is shown, it can be said that the system also passed this security test.



Tese Mestrado
Fernando Vidal

Issued on Feb 25, 2020 by Universidade Fernando Pessoa

Format validation

Getting transaction ID
Computing local hash
Fetching remote hash

Error
Could not confirm the transaction

Figure 17: Block not yet confirmed

4 Conclusion

Diploma fraud is far from being over. The combat mechanisms proved to be extremely inefficient, mainly in the paper models. Digital degrees have evolved with digitalization, but they do not offer privacy to the students, so they can have confidence in freely distributing their certificates.

Blockchain's disruptive technology offers a breakthrough in distribution and ensures protection from tampering. It was also shown that the blockchain offers the best resources to act in case of loss or theft of the university's private key, protecting the entity against undue retroactive emissions. Besides, the level of privacy offered by the technology, by recording only the hash certificate on the blockchain, makes the solution less prone to data leakage than the digital certificate solutions without blockchain.

The materialization of the objective of using the blockchain for the management of diplomas was achieved during the construction of the CertEdu prototype, in which it was possible to operate issuances, revocations, shares, and verifications of academic certificates.

However, tests also pointed out that disconnected operation is still an issue that needs to be worked on. Although some blockchains already offer resources, such as the smart contract, which would allow to easily resolve the centralization points placed, the premise of the solution operating on any type of blockchain has not been met, so those issues that still prevent decentralization are still raised by this work is pending.

There is also concern about the unpredictability of the issuance costs. Thinking of public networks like Bitcoin and Ethereum, you cannot predict the rate of transactions in the long run. This issue can inhibit the adhesion of universities.

Finally, it is concluded that the application of blockchain in the management of academic certificates is perfectly possible and that the technology already offers benefits in terms of privacy, distribution and revocation, compared to digital solutions. However, to be able to take advantage of the full potential of the technology, the centralization points addressed by this work, such as the validation of the issuer's profile and revocation, need to be migrated to features that operate within the blockchain itself.

Conflict of Interest The authors declare no conflict of interest.

Acknowledgment The authors acknowledge the support of DuoTi Solucoes.

References

[1] F. Vidal, F. Gouveia, C. Soares, "Analysis of Blockchain Technology for Higher Education," in 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 28–33, IEEE, 2019, doi:10.1109/CyberC.2019.00015.

[2] N. Smolenski, D. Hughes, Academic Credentials in an Era of Digital Decentralization, Learning Machine Research, Anaheim, CA, 2016.

[3] IBGE, "Rendimento médio real mensal do trabalho principal, por níveis de instrução," 2018.

[4] M. Oliver, J. Moreno, G. Prieto, D. Benitez, "Using blockchain as a tool for tracking and verification of official degrees: business model," in Using blockchain as a tool for tracking and verification of official degrees: business model, 29th European Regional Conference of the International Telecommunications Society (ITS): "Towards a digital future: Turning technology into markets?", Trento, Italy, 1st - 4th August 2018, International Telecommunications Society (ITS), Trento, 2018.

[5] F. R. Vidal, F. Gouveia, C. Soares, "Revocation Mechanisms for Academic Certificates Stored on a Blockchain," in 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 1–6, IEEE, Sevilha, 2020, doi:10.23919/CISTI49556.2020.9141088.

[6] F. Schär, M. Fabian, "Blockchain diplomas: Using smart contracts to secure academic credentials," Beiträge zur Hochschulforschung, **48**, 2019.

[7] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Www.Bitcoin.Org, 2008, doi:10.1007/s10838-008-9062-0.

[8] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," IEEE Access, 2018, doi:10.1109/ACCESS.2018.2789929.

[9] M. Saad, J. Spaulding, L. Njilla, C. A. Kamhoua, S. Shetty, D. Nyang, A. Mohaisen, "Exploring the Attack Surface of Blockchain: {A} Systematic Overview," CoRR, **abs/1904.0**, 2019.

[10] J. a. Kroll, I. C. Davey, E. W. Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries," The Twelfth Workshop on the Economics of Information Security (WEIS 2013), 2013, doi:June11-12,2013.

[11] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Crypto-Currencies, O'Reilly Media, Inc., 1st edition, 2014.

[12] R. C. Merkle, "A digital signature based on a conventional encryption function," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1988, doi:10.1007/3-540-48184-2 32.

[13] L. M. Palma, M. A. G. Vigil, F. L. Pereira, J. E. Martina, "Blockchain and smart contracts for higher education registry in Brazil," International Journal of Network Management, **29**(3), e2061, 2019, doi:10.1002/nem.2061.

[14] D. Yaga, P. Mell, N. Roby, K. Scarfone, "Blockchain technology overview," Technical report, National Institute of Standards and Technology, Gaithersburg, MD, 2018, doi:10.6028/NIST.IR.8202.

[15] A. Grech, A. F. Camilleri, Blockchain in Education, Publications Office of the European Union, 2017, doi:10.2760/60649.

[16] H. Haugsbakken, I. Langseth, "The Blockchain Challenge for Higher Education Institutions," European Journal of Education, **2**(3), 2019.

[17] N. Bore, S. Karumba, J. Mutahi, S. S. Darnell, C. Wayua, K. Weldemariam, "Towards Blockchain-enabled school information hub," in ACM International Conference Proceeding Series, 2017, doi:10.1145/3136560.3136584.

[18] A. Ronning, W. W. Chung, "Blockcerts V3 Proposal," 2019.

[19] M. L. MIT Media Lab, "Blockcerts-An Open Infrastructure for Academic Credentials on the Blockchain," 2016.

[20] M. Bartoletti, L. Pompianu, "An analysis of Bitcoin OP-RETURN metadata," CoRR, **abs/1702.0**, 2017.

[21] J. C. Cheng, N. Y. Lee, C. Chi, Y. H. Chen, “Blockchain and smart contract for digital certificate,” in Proceedings of 4th IEEE International Conference on Applied System Innovation 2018, ICASI 2018, 2018, doi: 10.1109/ICASI.2018.8394455.

[22] T. Kanan, A. T. Obaidat, M. Al-Lahham, “SmartCert BlockChain Imperative for Educational Certificates,” in 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), 629–633, IEEE, 2019, doi:10.1109/JEEIT.2019.8717505.

[23] K. Mori, H. Miwa, “Digital university admission application system with study documents using smart contracts on blockchain,” in Advances in Intelligent Systems and Computing, 2020, doi:10.1007/978-3-030-29035-1_17.

[24] K. Patel, M. L. Das, “Transcript Management Using Blockchain Enabled Smart Contracts,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2020, doi:10.1007/978-3-030-36987-3_26.

[25] M. Jirgensons, J. Kapenieks, “Blockchain and the Future of Digital Learning Credential Assessment and Management,” Journal of Teacher Education for Sustainability, 2018, doi:10.2478/jtes-2018-0009.

[26] C. Iragorri, “Academic certificates on Hyperledger,” 2018.

[27] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger. EIP-150 REVISION,” 2017, 2017.

[28] J. Santos, K. H. Duffy, “A Decentralized Approach to Blockcerts Credential Revocation,” 2019.

[29] L. Rujia, D. Galind, “BTCert,” 2017.

[30] R. Kumar, R. Tripathi, “Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain,” in 2019 Fifth International Conference on Image Information Processing (ICIIP), 246–251, IEEE, 2019, doi:10.1109/ICIIP47207.2019.8985677.

[31] S. Wang, Y. Zhang, Y. Zhang, “A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems,” IEEE Access, 2018, doi:10.1109/ACCESS.2018.2851611.

[32] A. Rajalakshmi, K. Lakshmy, M. Sindhu, P. Amritha, “A Blockchain and IPFS based framework for secure Research record keeping,” International Journal of Pure and Applied Mathematics, **119**(15), 2018.