EduCert – Blockchain-Based Management Information System for Issuing and Validating Academic Certificates

Diogo Melim[1] and António Trigo[1,2](✉)

[1] Polytechnic of Coimbra, Coimbra Business School Research Centre, Instituto Superior de Contabilidade e Administração de Coimbra (ISCAC), 3045-601 Coimbra, Portugal
antonio.trigo@gmail.com, a2016042046@alumni.iscac.pt
[2] Centro ALGORITMI, University of Minho, 4804-533 Guimarães, Portugal

Abstract. The forgery of academic certificates is a global concern, being one of the best-known examples the case of fake doctors. This counterfeiting is facilitated because the validation of these certificates by the employers is, in most cases, through visual inspection of the certificates which, by itself, does not guarantee their veracity. In this sense, this work proposes a new certification approach based on blockchain technology that allows anyone to validate an academic certificate by placing the hash or the pdf of the academic certificate in a web application that performs this validation in a public blockchain network, without the need to authenticate.

Keywords: Blockchain · Authentication · Certification · Academic Degree · Diplomas · Higher Education · Forgery

1 Introduction

The validation of the authenticity of records of academic degrees and diplomas is still an archaic process that resorts in most cases to visual validation of the same by the clerks of the various organizations whether they are issued on paper or in electronic format, which even having digital signatures, are easy to forge putting in question their veracity. If the organization's clerks responsible for validating the academic degrees doubt the authenticity of the documents, they will have to contact the Higher Education Institution (HEI), either by e-mail or by phone, which takes time and resources both for the organization that wants to hire a new professional and for the HEI that must validate the document.

In addition to the issue of the practicality of validating documents, there is also the issue of forged certificates of academic degrees and diplomas, which has reached considerable volumes in recent years, believed to reach billions of dollars [1], and it is easy to obtain online forged certificates from prestigious universities.

Considering the above, a decentralized, blockchain-based degree and diploma certification prototype (source code available at https://github.com/dmelim/EduCert) is proposed to solve this problem, which will allow any user anywhere in the world to validate

M. Papadaki et al. (Eds.): EMCIS 2022, LNBIP 464, pp. 137–149, 2023.
https://doi.org/10.1007/978-3-031-30694-5_11

whether the pdf document he or she holds, relating to a degree or diploma certificate issued by a HEI is valid.

The rest of the paper is structured as follows. In the next section a literature revision on the concepts and similar systems is presented. Next a section regarding the development of the system is presented. A section with the presentation of the application and some use cases is also provided. Finally, the paper ends with the conclusions section, where the limitations of the work and proposals for future work are presented, not only technical but also for the dissemination and promotion of the system developed.

2 Background

In this section introductory concepts about blockchains are presented as well as some examples of its use in the validation of academic degrees and diplomas found in the literature review.

2.1 Blockchain Concepts

Blockchain started as a concept rather than a term. It was introduced by Satoshi Nakamoto [2], an alias of the original creator of the concept, in October of 2008. This technology was developed to guarantee secure transactions between two parties without the need for a third party, thus creating the concept of trustless networks. The evolution of this technology has taken it to different domains beyond financial transactions, being considered today as one of the most important technologies of the present century [3].

Blockchain

A blockchain consists of data sets that are composed of a chain of blocks, where each block contains a timestamp, the hash value of the previous block and a nonce, which is a random number for hash verification, thus ensuring the integrity of the entire blockchain up to the first block [4]. As Satoshi Nakamoto has put in the original bitcoin paper, "Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it". [2].

The blockchain is distributed across several computers designated as nodes responsible for transactions and the addition of new blocks. Although there are different types of organization, this is originally a decentralized process where each node owns a copy of the blockchain and is rewarded for ensuring the functioning of the network [5]. To prevent network fraud, the original network of this concept, bitcoin uses a mechanism called proof-of-work [2], a decentralized consensus mechanism that requires network members to spend effort solving complex mathematical problems. This factor is a deterrent to actors who wish to threaten the network, as the computational power required to change a single block is enormous. Nakamoto came up with a principle that explains this concept well, "Proof-of-work is essentially one-CPU-one-vote" [2].

Given the high energy cost of maintaining a consensus mechanism using proof-of-work, other blockchain-based networks try to find other consensus mechanisms, being one of the most famous the proof-of-stake. In this mechanism members of the network instead of having to contribute to the network with their computational effort they contribute with the storage of network tokens in question. This mechanism assumes that if members of the network are required to store network tokens, they will not engage in fraudulent transactions that jeopardize their capital. As an example, the Ethereum network is migrating to this new mechanism by requiring members of the network to have a minimum of 32 ETH to participate in the network, which at current values is about $50,000. This consensus mechanism is being widely adopted in the recent years because, contrary to proof-of-work, it doesn't need computer power, and spends less electricity and so pollutes less [5].

Smart Contracts

Later Vitalik Buterin, decided to improve on the concepts created by Nakamoto, to create the Ethereum Blockchain. Buterin saw in Bitcoin more potential and along the years, the works of Nick Szabo, Namecoin, Colored coins and Metacoins inspired him to implement some ideas and developing them further [6].

One of these ideas was the implementation of smart contracts in the Ethereum network through a Turing complete programming language, which would make possible to build decentralized applications on Ethereum. Smart contracts are like normal contracts, an agreement between two or more parties, but instead of an entity checking if the conditions are completed, a computer automatically executes the contract when the conditions are met. This concept was introduced by Nick Szabo in the 1990's. [7].

To complete this objective Vitalik Buterin created Solidity, a smart contract programming language. Solidity makes it possible to work with the backend of Ethereum applications, also called Decentralized Applications, or DAPPS for short. This is a simple workflow in the Ethereum network [8].

Permission vs. Permissionless

There are two types of blockchains, private or permissionless and public or permissioned. Private blockchains restrict the users who can participate in transactions or the validation process. So only authorized users can participate in it. However private blockchains can have their history seen by external people to the network [9]. In contrast, public blockchains do not restrict anyone who wants to participate in the network or the validation process. Even so, the network can still have rules that need to be obeyed to participate in it [9].

2.2 Blockchain Certificate Authentication in Education

In the literature there are several experiences and studies about the application of BlockChain in the education area, in particular in the area of academic certificate management [10–16] Below are presented two projects whose characteristics were considered the most important for the development of the project presented in this paper.

Marella and Vijayan [11] developed a solution like the one proposed in this paper but based on a permissioned or private blockchain. Their problem was related to verifying the authenticity of the information stated on CV's. The authors chose to use Hyperledger Fabric [17], an open source blockchain technology that belongs to the permissioned or private blockchain subtype. Along with this they decided to use a consortium blockchain platform, which is a private blockchain that has a wider user base, for example instead of just one company using the blockchain, a group of organizations share this blockchain platform. To make it user friendly, a frontend, using, HTML and JavaScript was built. The information that is stored in the blockchain is the hash of the document, that can be calculated using an algorithm. For this they used the SHA-256 algorithm. Then this hash and the hash of the identification is stored in the blockchain as a message. To make the process easier 3 entities were created, the “peers”, “Administrators” and the “Certification Authority”. The peers take care of the process of submitting the hash to the blockchain. The administrator verifies the authenticity of the documents submitted and can approve or refuse their submission. The Certification Authority has the capability to give the certificates to the peers and administrators. The authors conclude this research presenting a comparison with a more traditional way of achieving this, using a central database application. The greatest reason they see to use blockchain instead is the immutability nature blockchain has. Giving it a layer of security and providing data integrity. Another reason is the scalability, in their case, it can have global impact, since hiring managers across the globe can check the information of candidates from various geographic locations [11].

Rama et al. [12] developed a software solution to identify fake or forged university credentials, using a decentralized application with Ethereum blockchain, using JavaScript and MetaMask to develop it. For the development phase they use Truffle and Ganache, a very useful set of tools made for the development of Decentralized Applications on Ethereum. To create the smart contract, Solidity was used. In their case, they propose that the blockchain is managed by a consortium of colleges and universities. If a student wants to use this to store their information, he or she needs to approach this consortium for approval. Certificates are given an individual identification, which is used as a verification mechanism.

3 Prototype

This section presents the development of the authentication system for academic degree and diploma certificates, from the enumeration of the requirements to be implemented to the actual coding, highlighting some of the codified components, presenting some of the screens of the front-end application for interaction with the blockchain where the hashes of the certificates are.

3.1 Requirements

The EduCert system is composed of two main packages. One that manages the entire cycle and life of degree and diploma certificates, which includes publishing their hash on the blockchain and registering them in the database. The other allows the management of users who have access to the platform, allowing the normal actions, such as their authentication in the system, registration/deletion of users and management of the respective permissions.

Figure 1 presents the use case diagram of the certificate management package. It was decided not to present the use case diagram relative to the user management package because the use cases are those commonly present in user management systems.

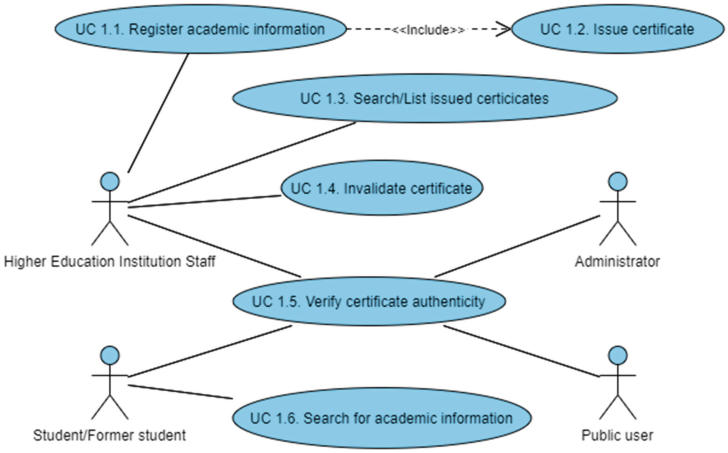

UC 1.1. Register academic information
<<Include>>
UC 1.2. Issue certificate
UC 1.3. Search/List issued certicicates
UC 1.4. Invalidate certificate
Higher Education Institution Staff
Administrator
UC 1.5. Verify certificate authenticity
Student/Former student
UC 1.6. Search for academic information
Public user

Fig. 1. Certificate management system use cases

The application as shown in Fig. 1 and Fig. 2 has four types of users: the HEI user, who manages the certificates in the system, having available the functionalities for registering the academic information in the system, which includes the issuing of certificates in the blockchain, the possibility to search the issued certificates and also invalidate the issued certificates (certificate invalidation can only be carried out in the database, not in the blockchain); the student user, who can consult his/her academic information including all the certificates issued by the different institutions of higher education; the public user who accesses the system to validate the certificates they have in their possession; and, finally, the administrator user who can perform in the system mainly operations related to the management of the users.

3.2 Architecture

As can be seen in Fig. 2 the EduCert system consists of an application server, where the frontend and backend are located, a database server and the blockchain network. The frontend allows the different users to interact with the system to perform different operations and communicate with the backend. The backend receives requests from the frontend through an Application Programmable Interface (API) to store information about students and their academic certificates both in the database and in the blockchain. The database stores all the information relative to the users and, in the case of the students, also the academic information including the certificates. Finally, the public blockchain where the hashes relative to the certificates are stored.

Given that the blockchain to be used in this project is public because the idea is that anyone wishing to verify if a certificate is valid can do so through the EduCert application or other, it becomes necessary to use a database to store more personal information that is not desired to be public in the blockchain. However, the information that is stored in the database has no influence on the verification of the authenticity of the certificates on the blockchain. They either exist in the blockchain or not.

The communication between the different users and the system components is as follows: the HEI user accesses the system to publish academic information relative to its students; the student user consults its academic information in the system, made available by the HEIs and delivers to the different institutions that need it, such as its work place, here designated as public user, the certificates or respective hashes, so that these users can consult in the system the veracity of these certificates.

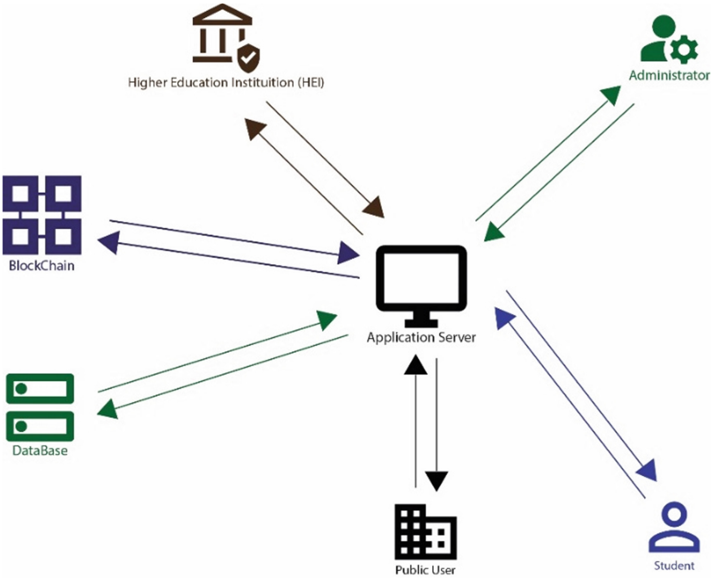


Fig. 2. EduCert architecture.

3.3 Technologies Used

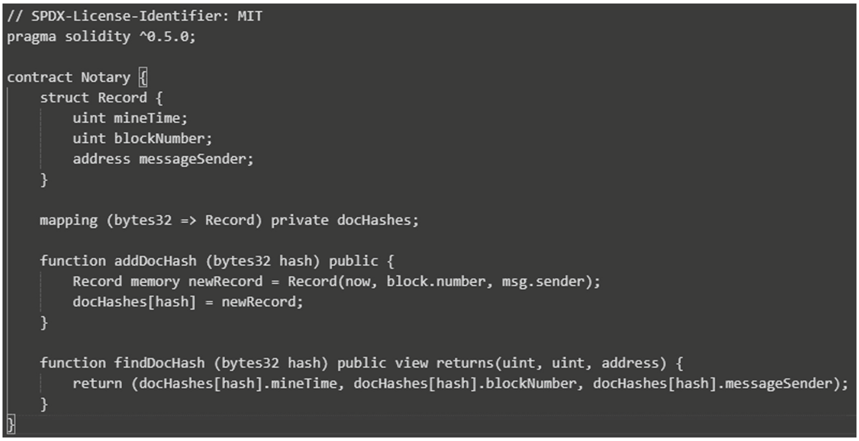
The following technologies were used to create the EduCert system:

- React/Express for building the frontend;
- NodeJS for building the back-end system, which communicates with the database and the blockchain and provides an API, to be used by the frontend, with a set of functionalities to perform the different operations both with the database and the blockchain;
- MongoDB as the database engine, for storing the information;

- Fantom blockchain, for storing certificate hashes. This blockchain was chosen because it has a lot of similarities with Ethereum and has smaller costs. The similarities like Ethereum allow the use of the tools available for Ethereum like writing the contracts in the Solidity language and using tools from the Ethereum ecosystem like Remix for compiling the contracts or Ganache for testing them.
- MetaMask, to store Fantom tokens and connect the browser to the blockchain to pay for the publishing fees of the hash certificates.
- Javascript language, used to program some of the above-mentioned technologies.

3.4 Implementation

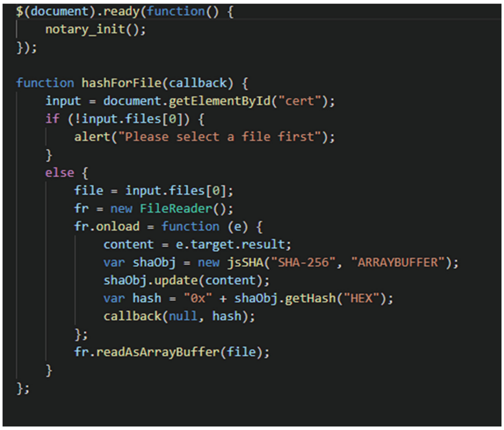
In this section some of the most important aspects of the coding of the EduCert system are presented, namely, the coding of the contract that sustains the publication of the certificates on the Fantom blockchain (Fig. 3), the example of the function of hash creation from the PDF file for validation on the blockchain (Fig. 4) and the backend functions for the publication (Fig. 5) and search/verification (Fig. 6) of the certificate validity, which are made available through the backend API. In the experimentation section of this document (Sect. 5) it is possible to see the visual part of the system made available to users through the front-end.



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.5.0;

contract Notary {
    struct Record {
        uint mineTime;
        uint blockNumber;
        address messageSender;
    }

    mapping (bytes32 => Record) private docHashes;

    function addDocHash (bytes32 hash) public {
        Record memory newRecord = Record(now, block.number, msg.sender);
        docHashes[hash] = newRecord;
    }

    function findDocHash (bytes32 hash) public view returns(uint, uint, address) {
        return (docHashes[hash].mineTime, docHashes[hash].blockNumber, docHashes[hash].messageSender);
    }
}
```

Fig. 3. Smart contract (solidity).

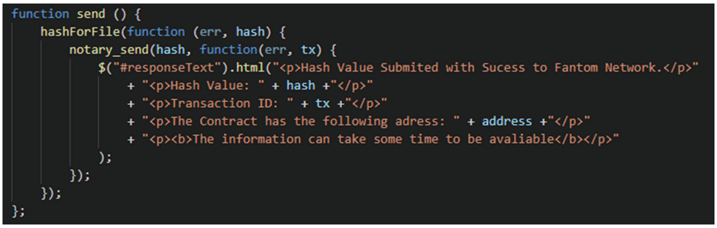
In Fig. 3 the smart contract code written for EduCert is presented, where it is possible to see the types of data involved (stamp, block number and the sender) as well as the functions that manipulate them (addDocHash and findDocHash). This contract was originally found in "Ether doc cert" GitHub repository [18]. To store a hash the user needs to pay gas fees, but to search it the user does not.



```
$(document).ready(function() {
    notary_init();
});

function hashForFile(callback) {
    input = document.getElementById("cert");
    if (!input.files[0]) {
        alert("Please select a file first");
    }
    else {
        file = input.files[0];
        fr = new FileReader();
        fr.onload = function (e) {
            content = e.target.result;
            var shaObj = new jsSHA("SHA-256", "ARRAYBUFFER");
            shaObj.update(content);
            var hash = "0x" + shaObj.getHash("HEX");
            callback(null, hash);
        };
        fr.readAsArrayBuffer(file);
    }
};
```

Fig. 4. Hashing algorithm.

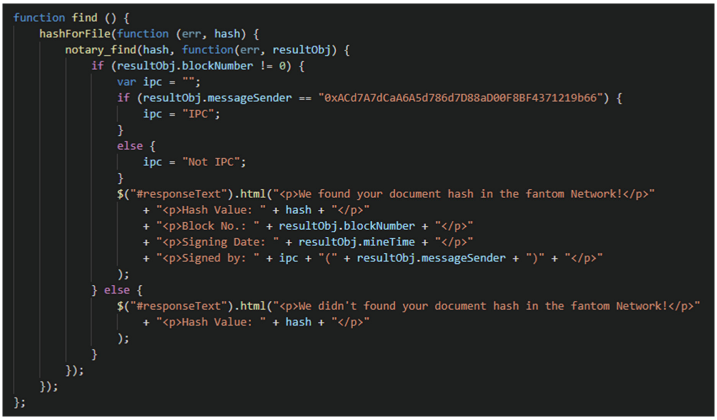
Figure 4 presents the hashing algorithm that calculates the hash of the file (PDF certificate of the academic degree), using a JavaScript library that uses an algorithm, in this case SHA-256 to calculate the hash of a document, which will be the hash stored on the blockchain (see Fig. 5).



```
function send () {
    hashForFile(function (err, hash) {
        notary_send(hash, function(err, tx) {
            $("#responseText").html("<p>Hash Value Submited with Sucess to Fantom Network.</p>"
                + "<p>Hash Value: " + hash +"</p>"
                + "<p>Transaction ID: " + tx +"</p>"
                + "<p>The Contract has the following adress: " + address +"</p>"
                + "<p><b>The information can take some time to be avaliable</b></p>"
            );
        });
    });
};
```

Fig. 5. Send hash to blockchain.

Figure 5 shows the method used to send the hash to the Fantom blockchain. This is done using the function "addDocHash" defined in the smart contract (Fig. 3) and a third-party module called Web3 [19]. This module makes it able to create functions that can interact with function inside a smart contract. In this case the "notary_send" function. This is linked to Metamask [20] which will signal to the user that a transfer is being attempted, which will be carried out, if the user agrees to it. This is also done through the web3.js Ethereum API library [19].



```
function find () {
    hashForFile(function (err, hash) {
        notary_find(hash, function(err, resultObj) {
            if (resultObj.blockNumber != 0) {
                var ipc = "";
                if (resultObj.messageSender == "0xACd7A7dCaA6A5d786d7D88aD00F8BF4371219b66") {
                    ipc = "IPC";
                }
                else {
                    ipc = "Not IPC";
                }
                $("#responseText").html("<p>We found your document hash in the fantom Network!</p>"
                    + "<p>Hash Value: " + hash + "</p>"
                    + "<p>Block No.: " + resultObj.blockNumber + "</p>"
                    + "<p>Signing Date: " + resultObj.mineTime + "</p>"
                    + "<p>Signed by: " + ipc + "(" + resultObj.messageSender + ")" + "</p>"
                );
            } else {
                $("#responseText").html("<p>We didn't found your document hash in the fantom Network!</p>"
                    + "<p>Hash Value: " + hash + "</p>"
                );
            }
        });
    });
};
```

Fig. 6. Searching function.

The function presented in Fig. 6 searches the Fantom blockchain for the corresponding hash. It starts by verifying if the message sender, or the account that uploaded the hash originally, is a valid account. The value is hard coded, as this is a prototype. If it is an authorized account, it gives the user who searched for the hash more information about it. If it isn´t it notifies the user of it. If the hash is not on the network, the user will be notified with a different message.

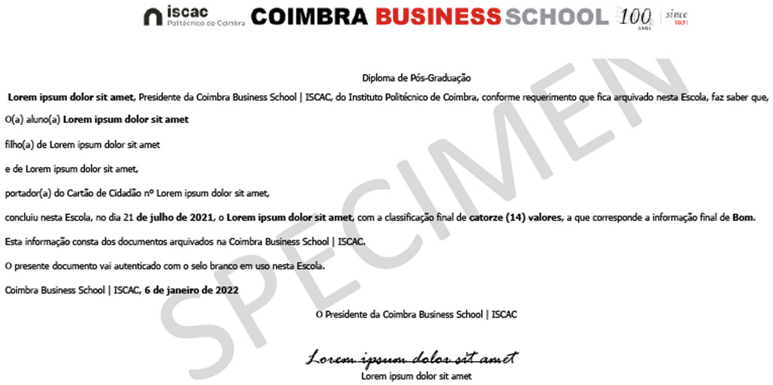
4 Exemplification of Prototype Use

In this section two use cases of the EduCert system are presented, that of issuing an academic certificate by the HEI and that of validating the certificate by a public user (e.g., a user from a company where the former student/student is applying for a job).

4.1 HEI Issue Certificate

An administrative employee from HEI, in this example, Coimbra Business School from the Polytechnic of Coimbra, Portugal, accesses the system to issue an academic certificate relative to a student. To do so, he or she fills in a form with the necessary information to issue the certificate, which, after validated, will be used to generate the certificate. There is also the option of importing from Excel the information relative to several students for the issuing of the certificate.

After sending this information, the certificate in PDF is generated by the EduCert system (see Fig. 7) and the respective hash is calculated for storage in the Fantom blockchain.


iscac Politécnico de Coimbra
COIMBRA BUSINESS SCHOOL
100 anos
since 1921
SPECIMEN

Diploma de Pós-Graduação

Lorem ipsum dolor sit amet, Presidente da Coimbra Business School | ISCAC, do Instituto Politécnico de Coimbra, conforme requerimento que fica arquivado nesta Escola, faz saber que,

O(a) aluno(a) **Lorem ipsum dolor sit amet**

filho(a) de Lorem ipsum dolor sit amet

e de Lorem ipsum dolor sit amet,

portador(a) do Cartão de Cidadão nº Lorem ipsum dolor sit amet,

concluiu nesta Escola, no dia 21 **de julho de 2021**, o **Lorem ipsum dolor sit amet**, com a classificação final de **catorze (14) valores**, a que corresponde a informação final de **Bom**.

Esta informação consta dos documentos arquivados na Coimbra Business School | ISCAC.

O presente documento vai autenticado com o selo branco em uso nesta Escola.

Coimbra Business School | ISCAC, **6 de janeiro de 2022**

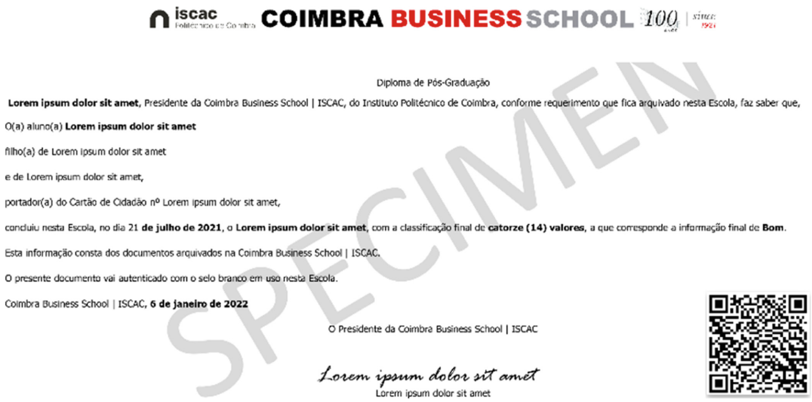
O Presidente da Coimbra Business School | ISCAC

Lorem ipsum dolor sit amet

Lorem ipsum dolor sit amet

Fig. 7. PDF certificate example

After generating the certificate, the system asks the user if he/she wants to open the MetaMask to complete the transaction. If the user authorizes the hash of the original certificate is stored in the Fantom blockchain and a new PDF certificate (see Fig. 8) similar to the previous one, but with a QR Code that contains the web address, with the hash of the original certificate, for validation, is generated.


iscac Politécnico de Coimbra
COIMBRA BUSINESS SCHOOL
100 anos
since 1921
SPECIMEN

Diploma de Pós-Graduação

Lorem ipsum dolor sit amet, Presidente da Coimbra Business School | ISCAC, do Instituto Politécnico de Coimbra, conforme requerimento que fica arquivado nesta Escola, faz saber que,

O(a) aluno(a) **Lorem ipsum dolor sit amet**

filho(a) de Lorem ipsum dolor sit amet

e de Lorem ipsum dolor sit amet,

portador(a) do Cartão de Cidadão nº Lorem ipsum dolor sit amet,

concluiu nesta Escola, no dia 21 **de julho de 2021**, o **Lorem ipsum dolor sit amet**, com a classificação final de **catorze (14) valores**, a que corresponde a informação final de **Bom**.

Esta informação consta dos documentos arquivados na Coimbra Business School | ISCAC.

O presente documento vai autenticado com o selo branco em uso nesta Escola.

Coimbra Business School | ISCAC, **6 de janeiro de 2022**

O Presidente da Coimbra Business School | ISCAC

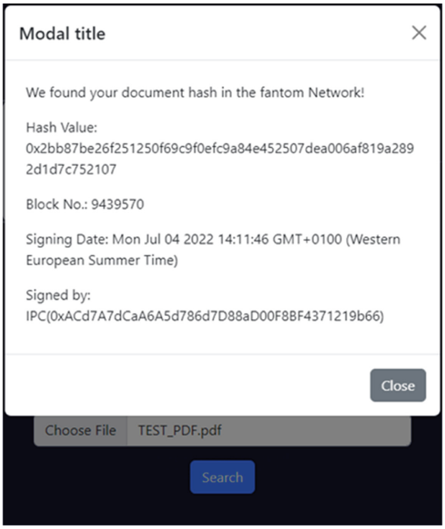
Lorem ipsum dolor sit amet

Lorem ipsum dolor sit amet

Fig. 8. PDF receipt certificate with QR Code

4.2 Verification of the CERTIFICate's Authenticity by the Public User

To verify the authenticity of a certificate issued by an HEI, the public user (e.g., a user from a company where the former student/student is applying for a job) takes a picture of the QR Code (see Fig. 8) that will take him to a web page of the EduCert system and tell him if the certificate in question is valid or not (see Fig. 9).



Modal title

We found your document hash in the fantom Network!

Hash Value:
0x2bb87be26f251250f69c9f0efc9a84e452507dea006af819a289
2d1d7c752107

Block No.: 9439570

Signing Date: Mon Jul 04 2022 14:11:46 GMT+0100 (Western
European Summer Time)

Signed by:
IPC(0xACd7A7dCaA6A5d786d7D88aD00F8BF4371219b66)

Fig. 9. EduCert system certificate search result

5 Conclusion

This paper presents the system developed for the validation of academic degree certificates, the EduCert system. This application has several components, with emphasis on the frontend where applications were created for interaction with different users (HEI, students and public or external users (who do not require authentication)) and the back-end component that records in the database the different operations performed and in the Fantom blockchain the certificate hashes.

In the testing phase, the system proved to be functional, being now necessary to test it in a real context. Nevertheless, some limitations have already been detected for which it will be necessary to find solutions, such as the immutability of the blockchain, which does not allow deleting records. In other words, although records are marked as invalid in the database, the same cannot be done at the blockchain level. These will always be occasional situations, because as in the case of physical certificates, once issued they are valid.

As future work there are, as already mentioned, tests at the level of the teaching institution where this solution was developed, the Polytechnic of Coimbra and, in the future, try to extend the use of this solution to other institutions.

As a conclusion would like to leave a summary of the costs per certificate to have such a system. In the case of Fantom blockchain, chosen for this stage of the system, the costs are about 0.026 FTM ($\approx$ 0.001 euros), while if chosen the Ethereum network are about 0.12 euros. The Ethereum network may be the option for the final system because it gives more guarantees of future support, i.e., that it will not disappear as a platform. Added to this is the fact that the Ethereum network is looking for a new consensus mechanism (proof-of-stake) that will lower transaction prices (gas fees costs) which will make the system even cheaper.

References

1. Grolleau, G., Lakhal, T., Mzoughi, N.: An introduction to the economics of fake degrees. J. Econ. Issues **42**(3), 673–693 (2008). https://doi.org/10.1080/00213624.2008.11507173
2. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org (2008). Accessed: 29 Mar 2022
3. el Haddouti, S., Ech-Cherif El Kettani, M.D.: Analysis of identity management systems using blockchain technology. In: Proceedings - 2019 International Conference on Advanced Communication Technologies and Networking, CommNet 2019 (2019). https://doi.org/10.1109/COMMNET.2019.8742375
4. Nofer, M., Gomber, P., Hinz, O., Schiereck, D.: Blockchain. Bus. Inf. Syst. Eng. **59**(3), 183–187 (2017). https://doi.org/10.1007/S12599-017-0467-3/TABLES/1
5. Kim, C.: Ethereum 2.0: How it works and why it matters (2020)
6. Buterin, V.: A next generation smart contract & decentralized application platform. https://translatewhitepaper.com/wp-content/uploads/2021/04/EthereumOrijinal-ETH-English.pdf (2013). Accessed 12 Apr 2022
7. Zheng, Z., et al.: An overview on smart contracts: challenges, advances and platforms. Futur. Gener. Comput. Syst. **105**, 475–491 (2020). https://doi.org/10.1016/J.FUTURE.2019.12.019
8. Dannen, C.: Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners. Apress, Berkeley, CA (2017). https://doi.org/10.1007/978-1-4842-2535-6
9. Solat, S., Calvez, P., Naït-Abdesselam, F.: Permissioned vs. Permissionless Blockchain: how and why there is only one right choice. J. Softw. **16**, 95–106 (2021). https://doi.org/10.17706/jsw.16.3.95-106
10. Nguyen, B.M., Dao, T.C., Do, B.L.: Towards a blockchain-based certificate authentication system in Vietnam. PeerJ. Comput. Sci. **6**, 266 (2020). https://doi.org/10.7717/PEERJ-CS.266
11. Marella, V., Vijayan, A.: Document verification using blockchain for trusted CV information. In: AMCIS 2020 Proceedings. https://aisel.aisnet.org/amcis2020/adv_info_systems_research/adv_info_systems_research/12 (2020). Accessed 27 Mar 2022
12. Rama Reddy, T., Prasad Reddy, P.V.G.D., Srinivas, R., Raghavendran, C.V., Lalitha, R.V.S., Annapurna, B.: Proposing a reliable method of securing and verifying the credentials of graduates through blockchain. EURASIP J. Inf. Secur. **2021**(1), 1–9 (2021). https://doi.org/10.1186/s13635-021-00122-5
13. Alshahrani, M., Beloff, N., White, M.: Towards a blockchain-based smart certification system for higher education: an empirical study. Int. J. Comput. Dig. Syst. **11**(1), 553–571 (2022). https://doi.org/10.12785/ijcds/110145
14. Serranito, D., Vasconcelos, A., Guerreiro, S., Correia, M.: Blockchain ecosystem for verifiable qualifications. In: 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), pp. 192–199 (2020). https://doi.org/10.1109/BRAINS49436.2020.9223305
15. Bahrami, M., Movahedian, A., Deldari, A.: A comprehensive blockchain-based solution for academic certificates management using smart contracts. In: 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE), pp. 573–578 (2020). https://doi.org/10.1109/ICCKE50421.2020.9303656

16. University of Nicosia: Blockchain Certificates (Academic & Others). https://www.unic.ac.cy/iff/blockchain-certificates/ (2014). Accessed 10 Sep 2022
17. Hyperledger Foundation, "Hyperledger Fabric". https://www.hyperledger.org/use/fabric (2022). Accessed 12 Apr 2022
18. Dat Tran, "Ether doc cert," GitHub. https://github.com/datts68/ether-doc-cert (2022). Accessed 19 Jul 2022
19. ChainSafe: "Web3.js," Git Hub. https://github.com/ChainSafe/web3.js (2014). Accessed 20 Jul 2022
20. MetaMask: Metamask-extension. https://github.com/MetaMask/metamask-extension (2019). Accessed 20 Jul 2022