Instituto Superior de Contabilidade e Administração

Politécnico de Coimbra

Instituto Superior de Contabilidade e Administração

Politécnico de Coimbra

EduCert – Blockchain prototype for authentication of academic degrees and certificates

Diogo Melim

ISCAC | 2022

Instituto Superior de Contabilidade e Administração

Politécnico de Coimbra

Diogo Melim

EduCert – Blockchain prototype for authentication of academic degrees and certificates

Coimbra, agosto de 2022

Instituto Superior de Contabilidade e Administração
Politécnico de Coimbra
COIMBRA BUSINESS SCHOOL
ISCAC.pt

Diogo Melim

EduCert – Blockchain prototype for authentication of academic degrees and certificates

Trabalho de projeto submetido ao Instituto Superior de Contabilidade e Administração de Coimbra para cumprimento dos requisitos necessários à obtenção do grau de **Mestre em Análise de Dados e Sistemas de Apoio à Decisão**, realizado sob a orientação do Doutor António Trigo.

Coimbra, agosto de 2022

TERMO DE RESPONSABILIDADE

Declaro ser o autor deste projeto, que constitui um trabalho original e inédito, que nunca foi submetido a outra Instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas e que tenho consciência de que o plágio constitui uma grave falta de ética, que poderá resultar na anulação do presente projeto.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

ACKNOWLEDGEMENTS

In big projects there is always a sense of gratitude to everyone who supported me and helped me throughout the challenges.

I would like to start by thanking my advisor Doutor António Trigo. His support and patience in the development of the project was an essential key to unlock some harder parts of the project. It was difficult to maintain motivation and commitment through the writing and development, but sometimes having someone that motivates and displays fortitude in face of problems can be an inspiration and a deciding factor in finishing a project. For all these reasons a big thank you is in order.

I would also be grateful to my friend for all the support in concluding my objectives, through a motivational word or sometimes a much-needed leisurely moment. And other times understanding my absence.

Finally, I would like to acknowledge my parents. The economical and emotional burden that is having a son studying far from home, especially coming from the small Madeira Island is a big sacrifice. For all the years they invested in my education, helping, and incentivizing the pursuit of a better future. And for aiding in the shaping of the person that I am today. Without their support none of this would have been possible.

“Gratitude makes sense of our past, brings peace for today, and creates a vision for tomorrow. “(Melody Beattie).

RESUMO

A fraude é um problema recorrente em várias indústrias. Ao longo dos anos várias pessoas têm tentado resolver esta situação, através do uso de novas tecnológico. Contudo, as situações de fraude também beneficiaram desta situação. Estas situações de fraude são particularmente interessantes na área do ensino superior. A fraude académica por vezes pode ter alguma complexidade, mas noutros casos pode ser explorada através da simplicidade ou até antiguidade dos processos das instituições do ensino superior. Sendo que a criação e uso de certificados falsos é um problema mundial. Muitas instituições em Portugal têm sistemas pouco, ou até nada, digitais. Isto deve-se a várias causas, algumas por falta de recursos para treinar os recursos humanos ou para melhorar os sistemas. Outras por acreditarem que têm um sistema bom, e logo não sentem a necessidade de o melhorar. Isto pode levar a um aproveitamento de entidades fraudulentas que desenvolveram técnicas para se aproveitar deste tipo de sistemas. Um sistema com apenas, certificados em papel, com assinaturas físicas não quer dizer que seja um sistema seguro. Para além da segurança a eficácia deste sistema também pode ser reduzida.

Contudo existe, nos dias de hoje, um consenso em que é necessária uma digitalização dos nossos sistemas. Várias empresas e pessoas já estão a trabalhar em algumas sugestões digitais, com o intuito de promover a facilidade de uso e de custo mantando a segurança e a digitalização. Estes dois fatores, segurança, para evitar a fraude, e digitalização para tornar os sistemas mais eficazes são fatores chaves. Uma das soluções, que tem se tornado nos últimos anos muito pertinente para várias indústrias é a blockchain. A blockchain tenta dar as instituições um sistema robusto, seguro e eficaz.

A solução apresentada por nós vai de acordo a estas necessidades, utilizando uma aplicação com recurso a blockchain. A nossa aplicação EduCert (https://github.com/dmelim/EduCert) usa a rede de teste da blockchain Fantom. A aplicação utiliza JavaScript para o seu frontend e backend. Para comunicar com a blockchain usamos Metamask, uma extensão do Google Chrome.

Palavras-chave: Blockchain, Certificados Digitais, Diplomas, Ensino Superior, Fraude Académica.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

ABSTRACT

Fraud is an issue that can occur in various industries. For a long time, different people and groups have tried to solve this problem, developing new solutions with the growing number of new technologies. However, new tech also helped frauds to become more numerous and complex. The fraud situations are particularly curious in the Higher Education field. Academic fraud is sometimes complex. Other times there are cases of fraud that takes advantage of older or simpler systems. The use and creation of fake certificates is a global issue. Most institutions in Portugal have system with a very low degree or even no digitalization. This is due to various causes, for example, low resources to improve human resources or informatic systems. Or even thinking that their system works as they want, and so there is no need to improve it. In turn, this can be exploited by fraudulent entities that develop techniques targeting these institutions. A system with only paper certificates and physical signatures doesn't translate to a safe system. Security isn't the only vulnerability these systems can have, they can also be inefficient.

Nevertheless, it exists a consensus in the academic community that there is a need for more digitalization. There are multiple entities working on digital solutions with the promise of a smooth transition. Security and digitalization are key factors to promote ease of use and increase efficiency. One of these solutions, is the use of a blockchain network. Blockchain can offer cohesion, efficiency, and security.

The solution that we present is in accordance with what we researched. The use of a blockchain system. Our application is EduCert (https://github.com/dmelim/EduCert), it uses the Fantom test blockchain. The application uses JavaScript for its frontend and backend. To communicate with the blockchain we use Metamask, a Google Chrome extension.

Keywords: Blockchain, Certification, Academic Degree, Diplomas, Higher Education, Forgery.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

ÍNDICE GERAL

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

ÍNDICE DE TABELAS E FIGURAS

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

LIST OFABBREVIATIONS AND ACRONYMS

API – Application Programming Interface

CPU – Central Processing Unit

CSS – Cascading Style Sheets

CV – Curriculum Vitae

DAO – Decentralized Autonomous Organization

DAPPS – Decentralized Applications

DASC – DAPP for Smart Certificates

DSR – Design Science Research

EJS – Embedded JavaScript Templating

eIDAS – Electronic Identification, Authentication and Trust Services

FTM – Fantom Currency

GO – Golang

HEI – Higher Education Institution

HR – Human Resources

HTTP – Hypertext Transfer Protocol

IPC - Polytechnic Institute of Coimbra

IPFS – Inter Planetary File System

IT – Information Technology

JS – JavaScript

JSON – JavaScript Object Notation

MOET – Ministry of Education and Training

QR Code – Quick Response Code

REST – Representational State Transfer

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

TLS – Transport Layer Security

UC – Use Case

URI – Uniform Resource Identifier

USB – Universal Serial Bus

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

1 INTRODUCTION

In the second year of the Master's in Data Analysis and Decision Supporting Systems the student decided to work on a project. This project enables for a self-paced practical work to put in practice the skills learned and learn new ones.

In the following sections we can find an overview of the developed project.

1.1 Background

The validation of the authenticity of certificates of academic degrees and diplomas is still a very archaic process that resorts, in most cases, to manual validation by the clerks of the various organizations, whether they are issued on paper or in electronic format. Even if there are digital signatures, they 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 (Grolleau et al., 2008), and it is easy to obtain online forged certificates from prestigious universities.

1.2 Objective

Considering the above, a decentralized, blockchain-based degree and diploma certification system is proposed to solve this problem, which will allow any user anywhere in the world to validate whether the pdf document s/he holds, relating to a degree certificate or diploma issued by a HEI, is valid. Making the work of human resources easier. For this to be possible, we plan to make an application which is easy to use, and that has all the functionalities regarding the use of blockchain. We plan to make is as simple as possible, due to the time and human resources constraints.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

1.3 Methodology

To develop the project, which is a web application, the Design Science Research (DSR) methodology was chosen. This methodology was chosen due to its nature to test solutions in a real-world context. This methodology also strives to improve the solutions iteratively. DSR has some guidelines that are derived from its core principles (Hevner et al., 2004):

1) Design as an Artifact: this guideline states that the research outcome must contemplate a valid artifact (some sort of model or method).
2) Problem Relevance: the significance of the solution is directly related to the problem it proposes to solve. The problems need to be important and relevant.
3) Design Evaluation: the design artifacts must be tested, and their utility demonstrated through well executed evaluations methods.
4) Research Contributions: the project must produce some contributions in the areas researched.
5) Research Rigor: the evaluation and constructions of the project must follow rigorous methods to maintain integrity.
6) Design as a search process: the means and researching process must satisfy laws in the problem environment.
7) Communication of Research: the presentation of the research must be easy to interpretate both by the technical and the managerial side.

In practice the stages that are part of the project can be interchangeable and repeated as many times as needed, what is advised is to keep the integrity of the above presented guidelines.

1.4 Project structure

This project is structured as follows. In chapter two we find a literature review. Here we can find some explanations to some core concepts of blockchain, then we go over some similar articles, in theme, that were found. In section three we go over the requirements of the project, then we review design concepts, like system architecture and the mockups built for our project. The used technologies and how we implemented, in terms of code, are also discussed in this section. In section four we review the final application. We

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

present screenshots of the application and go over some of the key features we implemented and how they are seen and interacted by the final user. Finally, we go over everything we have done and summarize the work, thinking about the limitations and how we can improve on it.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

2 LITERATURE REVIEW

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 was introduced by Satoshi Nakamoto (Nakamoto, 2008), a pseudonym 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. Blockchain is mainly used in the finance sector. However, the evolution of this technology has taken it to different domains beyond financial transactions, being considered as one of the most important technologies of the present century (Haddouti & Ech-Cherif El Kettani, 2019).

2.1.1 Blockchain

A blockchain consists of a data base that is composed of a chain of blocks. Each block contains a timestamp, the hash value of the previous block and a nonce. A nonce ("Number used once") is a random number for hash verification, that ensures the integrity of the entire blockchain up to the first block (Nofer et al., 2017). 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" (Nakamoto, 2008).

The blockchain is distributed across several computers designated as nodes. These are 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 (Kim, 2020).

To prevent network fraud bitcoin uses a mechanism called proof-of-work. As defined in Nakamoto work, "The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits." (Nakamoto, 2008).

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

A characteristic of proof-of-work is that computers need to solve complex mathematical equations. This value gets harder to find, the bigger the chain is, and the computer power needed also increases. So, if someone wants to make a branch with wrong information, it needs most nodes in the network to work on this branch and add blocks to expand. Eventually replacing the main one. But if we add the factor that for nodes to mine blocks and continue building a blockchain with fraudulent information, more computer power is needed. This factor is a deterrent to bad actors, because the power needed just to change the information in one block would be huge. Nakamoto came up with a principle that explains this concept well, "Proof-of-work is essentially one-CPU-one-vote" (Nakamoto, 2008).

The people that participate in this consensus are chosen depending on different factors and different networks. In bitcoin, everyone with a computer can participate, but the costs to maintain the computer power needed can get costly. In newer blockchains some new consensus mechanisms are being tried, for example proof-of-stake (Kim, 2020). In this mechanism, people instead of giving computer power, stake their native token. This staking processes involves freezing a certain quantity of tokens for a period, so instead of giving their computer power, they freeze their assets. If it was just that there would be nothing to win from making good decisions, and continuing a reliable main branch, so each time a node approves a good node they receive an extra number of tokens, in their staked amount. If they approve a block containing adulterated information, they can get punished by losing all or only a portion of their staked to-kens. 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 (Kim, 2020).

2.1.2 Smart contracts

Later Vitalik Buterin, decided to improve on the concepts created by Nakamoto, to create the Ethereum blockchain. Buterin wanted to improve on Bitcoin. With the works of Nick Szabo, Namecoin, Colored coins and Metacoins he was inspired to implement some ideas and developing them further (Buterin, 2013).

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

One of these ideas was the implementation of smart contracts in the Ethereum network through a Turing complete programming language[1], this would make it possible to build decentralized applications on Ethereum. Smart contracts are like normal contracts, an agreement between two or more people. However instead of an entity checking if the conditions are completed, a computer automatically executes de contract when the conditions are met. This concept was introduced by Nick Szabo in the 1990's (Zheng et al., 2020).

To complete this objective Buterin created Solidity, a smart contract programming language. The work of Chris Dannen gives a deeper insight to how Solidity works. This language is an amalgamation of Javascript and C that allows users and developers to create smart contracts and compile them to bytecode to then be processed by something called Ethereum Virtual Machine, which makes sure the contracts run when needed. Solidity makes possible to work with the backend of Ethereum applications, also called Decentralized Applications, or DAPPS for short (Dannen, 2017).

2.1.3 Permission vs. Permissionless

There are different 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 (Solat et al., 2021). In contrast, public blockchains do not restrict anyone who wants to participate in the network or the validation process. Nonetheless, the network can still have rules that need to be obeyed to participate in it (Solat et al., 2021).

2.2 Blockchain certificate authentication in Education

Some works already exist that show the use of blockchain technology in the educational field (Alshahrani et al., 2022; Marella & Vijayan, 2020; Nguyen et al., 2020; Reddy et

[1] A language that can run every program that a "Turing Machine" can run, like C, C++ or Java

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

al., 2021). The following paragraphs present some examples of the use of the blockchain for the validation of academic certificates.

2.2.1 Document verification using blockchain for trusted CV information

Marella & Vijayan (2020) developed a solution like the one proposed in this work, only based on a permissioned or private blockchain. Their problem was related to verifying the authenticity of the information stated on CV's and proceed to show studies confirming this. The authors choose to use Hyperledger Fabric (Hyperledger Foundation, 2022), 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 it´s 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 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 (Marella & Vijayan, 2020).

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

2.2.2 Proposing a reliable method of securing and verifying the credentials of graduates through blockchain

Reddy et al. (2021) 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 is 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.

2.2.3 Application of blockchain technology in online education

Sun et al. (2018) decided to do a deeper analysis into online education, more specifically massive open online courses. These types of courses have been a trend in recent years due to the easy accessibility and low prices the platforms giving these courses practice. But these platforms have their share of problems. For example, these courses tend to not be recognizable as official to companies and other institutions, and more of a way to check if the student have a certain knowledge in a specific field. However, it isn't a full proof of having it. The student's data privacy can also be at a risk because they are dependent on the security of a centralized platform. To solve this issue, the authors propose a solution using blockchain as a decentralized, distributed database. They also propose using smart contracts to manage some work normally done by people, for example, smart contracts can accept payments, settlements, and acceptance. This can be done almost immediately and with low costs due to the nature of smart contracts. This paper is more of a theoretical approach to solve the problem identified by the authors, there is no system in place, or any technology has been chosen. Nonetheless the idea is to create a smart, decentralized, and online education system.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

2.2.4 Towards a blockchain-based certificate authentication system in Vietnam

Nguyen et al. (2020) identified a big problem in Vietnam, the use and trade of fake certificates. To solve it they built a custom system named VECefblock, with the underlying layer being a blockchain, in this case Hyperledger Fabric, and then deploying it to Amazon EC2, a cloud service. The authors investigated blockchain systems and decided to go with it due to what they call the trust characteristic, which includes, transparency, data integrity, and the immutability feature.

The authors also found in related works that there are limitations regarding paper certificates, for example risk of forgery, loss, manual validity, and certificate recall can be solved with blockchain. Speaking more specifically of their problem, all the education and training at a national level is handled by the Ministry of Education and Training (MOET). Although there are exceptions to this, for example local governments or other ministries handling education and certification, which can make the process confusing and incur in duplication. To contribute to the situation there are no common databases managed by MOET or any other national agencies, with the information about the student and his results. This situation makes it easier to produce fake certificates as there is no valid source to truly verify it. The architecture of their system is the input-write-validate-seal.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

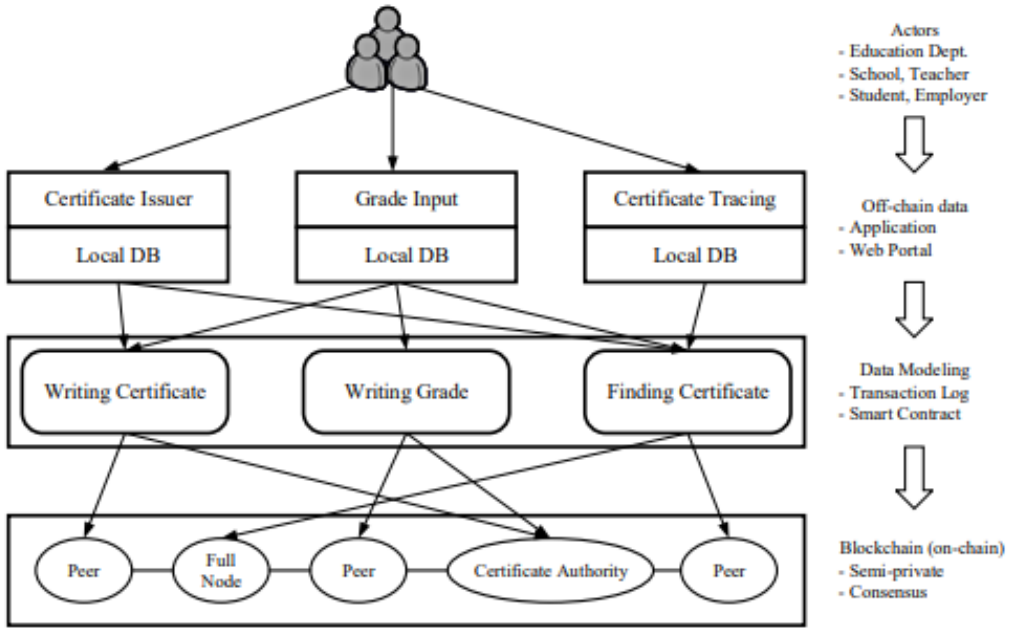

Figure 2.1. VECefblock system architecture

Source: Nguyen et al. (2020)

As we can see in Figure 2.1, they have 3 actors. The education Department, the school or teacher, and the student or the employer. These actors can interact with the system through the application or the web portal. The chosen blockchain is a semi-private. The data is modeled through the transaction log and the smart contracts.

The blockchain used is a permissioned one. The consensus model used is the Practical Byzantine Fault Tolerance (Nguyen et al., 2020). The objective is to give more control to MOET, as a central entity that verifies information sent by universities or other institutions.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

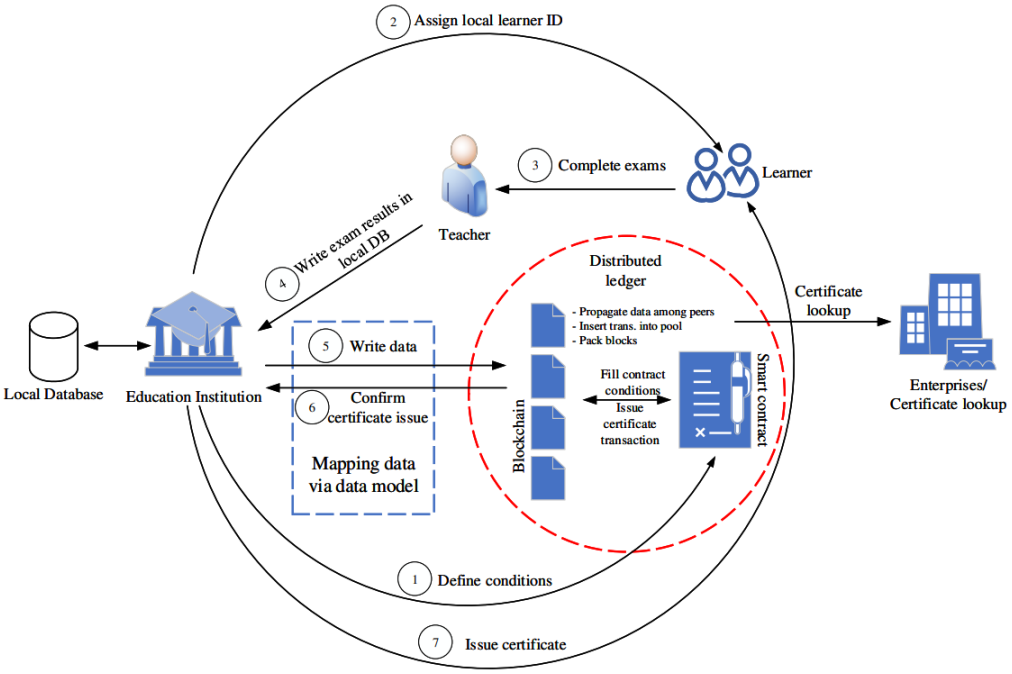

Figure 2.2. VECefblock business processes

Source: Nguyen et al. (2020)

Figure 2.2 shows a detailed view of the business processes of the system. These business processes show how the actors interact with the system, and how the data can travel across it.

As said before, they use Hyperledger as their blockchain layer, using JavaScript and NodeJS to develop their application.

The authors conclude with some ideas of future functionalities that they can implement. These functionalities are scaling up the application, with more nodes in different locations, building an effective query data mechanism, and performing analyses tests of the operability of VECefblock service when deploying on different sites.

2.2.5 Issuing and verifying digital certificates with blockchain

Another approach developed by Huynh et al. (2018) to solve a counterfeit certificates problem they identified globally, they used UniCoin, a blockchain. They used the metadata in transactions to store the hash of certificates using the Merkel Tree Hash Algorithm.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Their system flow gives us a general overview of their system, it goes as follows, the information is collected by the issuer to be certified, then the hash using the algorithm is stored in the metadata information, after that the transaction with this information is sent for validation, then the validation process is confirmed and the certificate owner receives the hash as an identity number that can be used to view certificates.

The Certificates are validated through the UniCert platform, to query for the information the identify number is needed with the transaction identity. Their architecture has the following flow, the users interact with the UniCert App, then the app application programming interface (API) communicates with the database, in this case PostgreSQL and the UniCoin Network. UniCoin is a blockchain developed by the authors, it uses proof-of-works as a consensus mechanism. The authors conclude that the system as a lot of advantages to prior non-blockchain systems, like the distributed nature and the immutability. To help developers and users they created the Unicoin platform and the Unicert application. The system makes it easy to perform the validity of certificates.

2.2.6 Towards a blockchain-based smart certification system for higher education: an empirical study

Authors Alshahrani et al. (2022) worked on a system to solve printed certificate fraud, costs of issuing certificates and time consumed to verify issued certificates. This system was applied in Higher education in Saudi Arabia. Their objectives when building this system were, to record student data like courses they registered in, credits, skills, and other relevant information, to share this data with authorized organizations, to help HEI share this data about their students, to help professors design and create unique teaching methods they can apply to specific student needs, to keep this information in a single repository that consolidates student information, and, finally to offer students the possibility to share their achievements and grades, like an internet portfolio.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

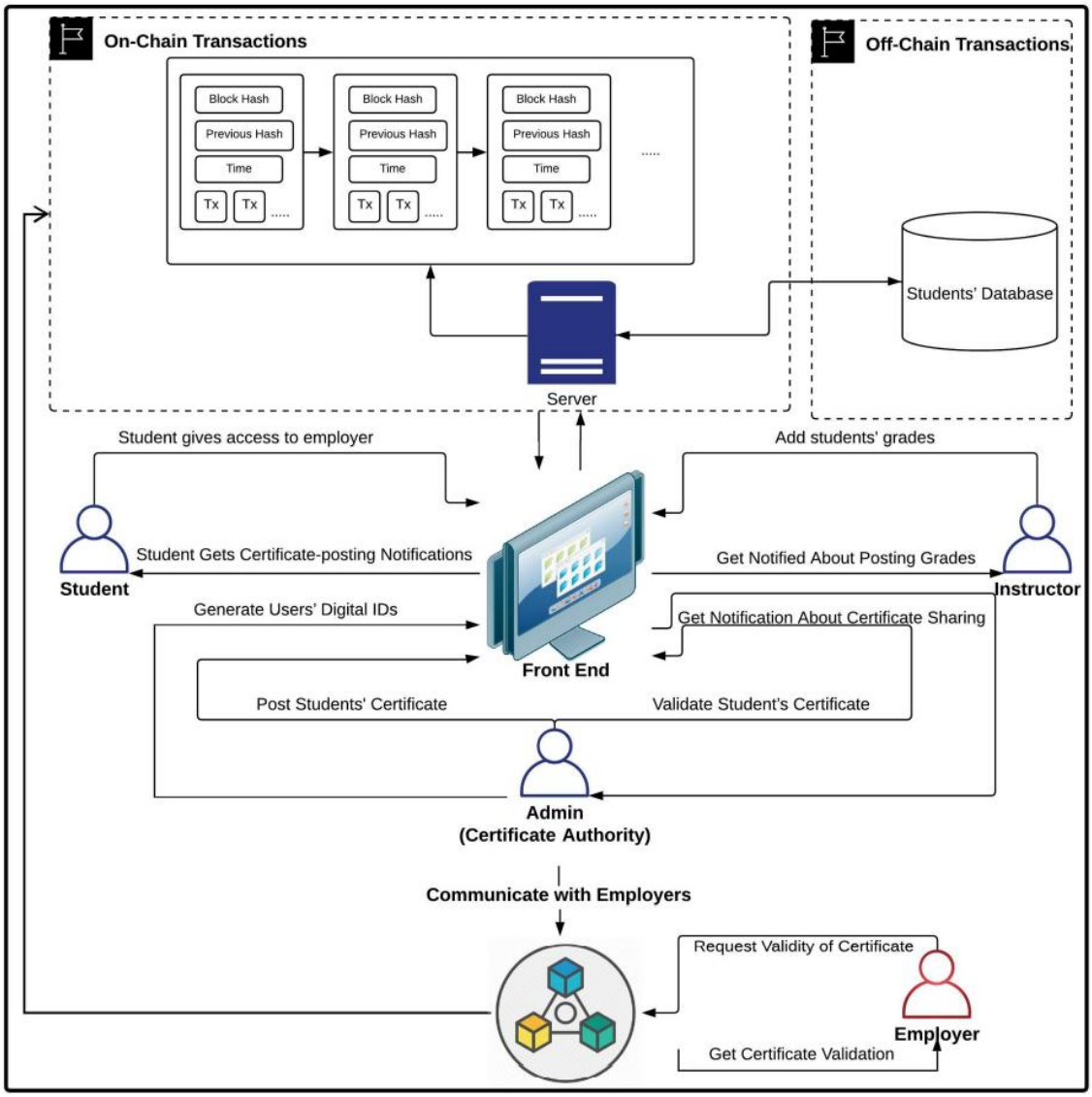

Figure 2.3. DASC system developed by Alshahrani

Source: Alshahrani et al. (2022)

The chosen systems follow the architecture shown in Figure 2.3. This system called DASC uses a blockchain based credential generating system that maintains student's credentials. The authors have not tested this system yet thus not being sure of its validity on a practical level, but for future works they will apply this system in a real case scenario.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

2.2.7 Design disclosure for blockchain-based application used in public education certificates with electronic hashes

Pfefferling and Kehling (2021) researched more than 30 academic publications related to certification in Education, and the development of the respective prototypes. After this research the investigators started to develop their own prototype.

The philosophy of their prototype is the Certificate as an object, which is the first layer. This certificate is attached to a single person, being created by a specific entity at a certain time. For the authors this relationship between the certificate, the person, and the entity that issued it is a trust anchor.

The second layer is the application layer, where the business logic is programmed, with user interfaces and machine interfaces. The prototype uses Java and RESTful APIs within the university network, and a separate sandbox with docker to allow cloud compatibility. Their "main driver" is https protocol with Transport Layer Security (TLS) encryption (Pfefferling & Kehling, 2021).

The third layer is centered on an USB card reader in combination with unique signatures. This is done to comply with the EU Electronic Identification, Authentication and Trust Services (eIDAS) regulations.

The blockchain in this project is used as the overarching for public connection and outside networks. The first blockchain they tried was Hyperledger Fabric in the cloud and later switched to a permissioned Ethereum-hybrid environment. They made this decision to attract more users and first public institutions on board. The data model for the blockchain is a combination of the SHA-256 hash of the PDF file, and three more variables, last name, birthday, and student ID, plus a random generated string as a pointer used in the verification process of the certificate itself. The authors conclude that in four years of academic works about blockchain there is no trend to a certain blockchain. They recommend further research to compare their proposed prototype solution to other prototypes to test how compatible it would be to novel and innovative technologies.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

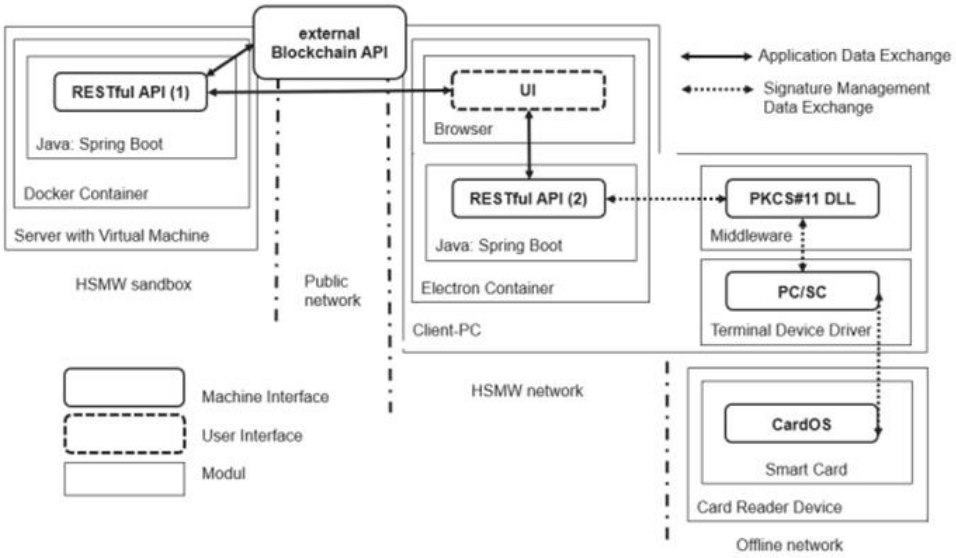

Figure 2.4. Pfefferling & Kehling system architecture

Source: Pfefferling & Kehling (2021)

2.2.8 Decentralizing certificates issuance through blockchain

Heredia et al. (2022) developed an interesting solution for certification in education and made it available for open-source users who want to try or improve it.

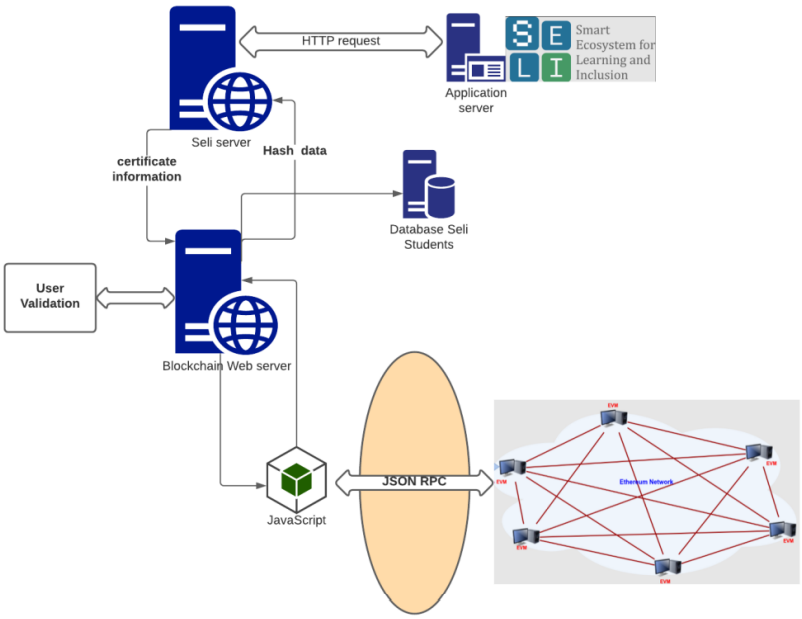

Figure 2.5. Heredia et al. system architecture.

Source: Heredia et al. (2022)

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

They describe their architecture and certificate generation process with 4 phases:

- First when the student has completed all his classes of a course and evaluations a request his sent, enabling the administrator to generate a certificate. In this case the administrator is the professor in charge of the student, the professor sends a request to the blockchain to store the student information on the blockchain.
- Then, once the information reaches the blockchain, if it's the first time this student has sent his information, an ID is given to his information. All the information needed is encrypted with AES-256 algorithm.
- Once the information has reached the blockchain server the student registration is validated and verified.
- Once this process is completed and the transaction information is given to the student, like a receipt, the corresponding hash is returned. Which is stored in the database and forwarded to their platform, called SELI. This information is assigned to the corresponding student.

The blockchain and backend used in their project is Go-Ethereum, written in Go (Golang). The Ethereum virtual machine which allows for the execution of the smart contracts is contacted using a Go backend (server). They also use Solidity, the primary smart contract language for the Ethereum ecosystem to write the contracts. Web3.js is also used, in conjunction with Go, which allows for an interaction with the blockchain, creating a client with diverse functionalities associated with blockchain interaction. And to conclude they used truffle.js, a framework that enable the creation of a testing ground for smart contracts and Ethereum decentralized application.

To better explain how their certificate generation and verification application works, they explain it with steps. The first one occurs when the student enrolls in the course through their platform and has completed it, the student will receive a notification with this information. Then, once the course is completed, the database is automatically updated, and the option to generate a certificate, in the professor dashboard, is enabled. Once this certificate is generated, the information is sent to the blockchain, and a certificate is generated in the blockchain network. Then the student is notified. Finally, when the notification link is clicked a new page is open. This page allows the verification of the

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

authenticity of the certificate through the hash. This link is publicly accessible and can be used by external entities for validation purposes.

The authors conclude that their systems guarantee information, precision, security, and ease of use for people who want to apply a digital contract model. The certification forgery is prevented by the hash plus content replication property. Students and teachers can access specific pages and utilities. The project being open source allows for easy improvements just by forking the project with GitHub. Their plans include some update for functionality of the project (Heredia et al., 2022).

2.2.9 CredenceLedger: a permissioned blockchain for verifiable academic credentials

Arenas & Fernandez (2018) bring to light a problem with the verification of academic credentials. They explain that places like "Recto U" can forge fake credential for a small cost, being a headache to companies and reputable universities. Due to this factor, they propose a solution using a permissioned blockchain, their argument for using it is the decentralization, immutability, security, and transparency characteristics. Their proposed solution is called CredenceLedger. It is based in Multichain a permissioned blockchain, to accompany this a mobile application was also developed. This allows the students to receive a paper or digital version of their credentials upon graduation. Decentralization and privacy are two of the focus of the authors when developing this solution.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

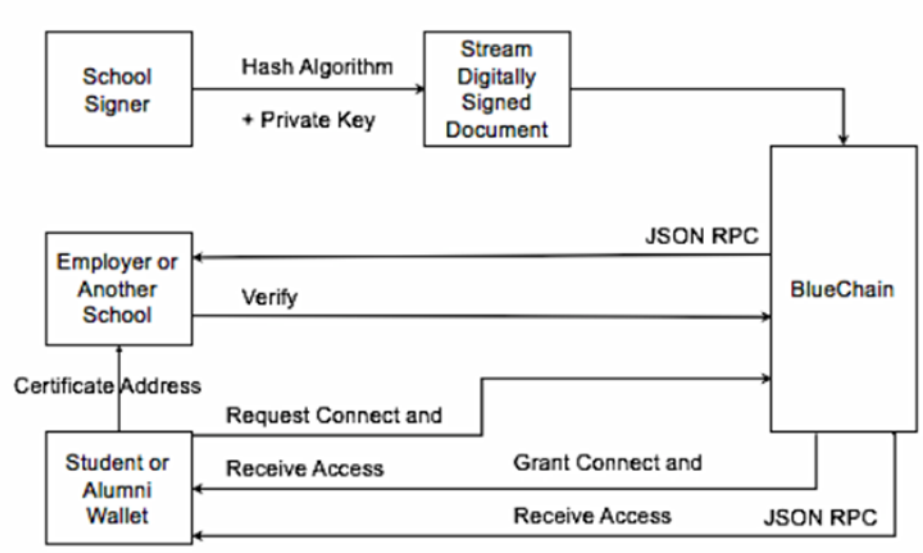

Figure 2.6. CredenceLedger Architecture

Source: Arenas & Fernandez (2018).

Their conclusion with the development of this project is that the availability of a digital version of the graduation certificate that can be verified helps employees more easily verify academic backgrounds. We can see their architecture in Figure 2.6. They also state that permissioned blockchains can be an effective distributed system in cases where multiple entities verify data without a need of a centralized database. This type of blockchain is also an efficient system for managing digital academic credentials, due to the high transaction output, and low costs and resources consumption.

2.2.10 Blockchain ecosystem for verifiable qualifications

In the Serranito et al. (2020) paper the problem of falsified or counterfeit certificates that is encountered by human resources contracting process is a worldwide situation. To try and present a solution to this the authors use blockchain, the attributes they deem important to solve this issue are decentralization, immutability, transparency, and security. Beyond this it also allows to cut the middleman, lowering the time and costs consumed.

The authors also state that their ecosystem may be considered a Decentralized Autonomous Organization (DAO), however, contrary to other DAO's they don't aim to

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

use or provide a cryptocurrency. Their ecosystem objective is to provide a service to recruiters and alumni.

This system has two main components to it. First the way that the actors interact with the blockchain, this component divide itself in three. One is a JavaScript application for each actor. The HEI client, that provides the capability to register or revoke certificates. The recruiter's app, that allows recruiters to verify the authenticity of the student's certificates. Finally, the Consortium App, that has a consortium-based voting system, that allows new HEIs to join. The other component is the smart contracts, they have two. One that enables the voting system, the consortium smart contract, that also allows the recruiters to get the HEI's smart contract address. Then there is the HEI Smart Contract, that is used by all entities to store or get certificate hashes. To better understand the flow of the information we can see Figure 2.7.

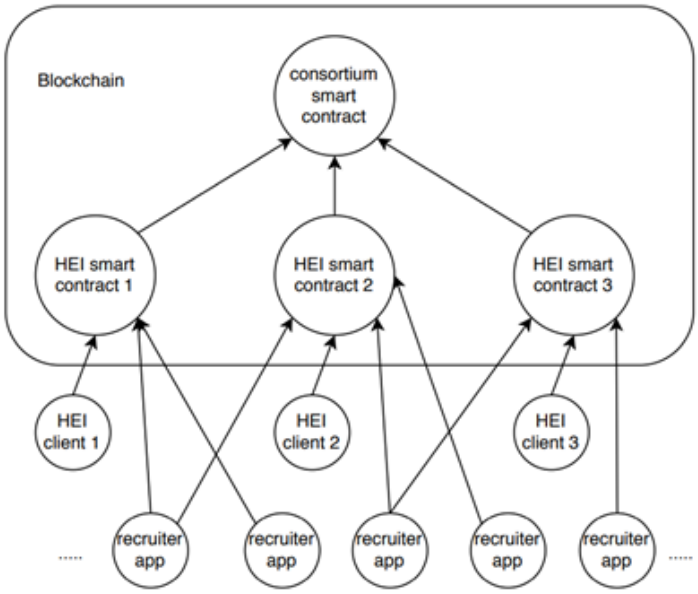

Figure 2.7. Data flow diagram, that represents the system developed with a consortium of 3 HEI as an example.

Source: Serranito et al. (2020)

To evaluate how their solution worked the authors used an Ethereum test net, to avoid increasing the costs unnecessarily. This testnet is called Ropsten, it was chosen because it resembles Ethereum main net the most. To make this test they chose three variables,

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Throughput, Costs, and Latency. The conclusions, of their test, are that using blockchain ends up being more efficient, less time consuming and cost free. It also gives employees the legitimacy and integrity of the process. The authors also desire that this project is used as a baseline to others develop on top and create a better and more robust solution on the future.

2.2.11 A framework to manage smart educational certificates and thwart forgery on a permissioned blockchain

Dumpeti & Kavuri (2021) also encountered a problem with the creation of fake certificates. After investigating, they decided to create a model using blockchain as a base, a method used by other institutions and researchers. For the authors the biggest advantages in using blockchain are that:

- The certificates are stored permanently using cryptographic methods, making the data near impossible to decode using current technology.
- Any modification is stored on the chain, making it possible to trace them on a later date.
- It's possible to verify the information with any of the available nodes.
- Reducing the costs by eliminating the need for a third party.
- To access the certificates a private key is needed.
- Companies can feel more safe hiring without the need to an increase in the investigation time.

The model developed by the authors uses Hyperledger fabric as blockchain, with internet of things integration, to make it easy for stakeholders to access it. They have different reasons to use Hyperledger Fabric, for example the transparency, the possibility to create multiple channels, where authorized organizations can join them, and each channel has its own distributed ledger. The permissions can be fined tuned for every case. The certificate authority makes it possible to give certificates so people can join. And, Hyperledger has a better throughput, execution time and latency compared to other blockchains.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

The system works as follows, a hash is generated from the certificate, and both items are stored together. Then the student is given a proof of the issuance of the certificate and a way to access it. Then the student can give it to the company and the company can check whether the certificate is valid or not.

To use Hyperledger there is no need to use a currency, so there are no costs related to the transfers. The authors conclude that their system is tamper proof and say that it is an efficient system, with fast transactions, authentication, user friendly and with the capability to fine tune the permissions (Dumpeti & Kavuri, 2021b).

2.2.12 Digital certificate system for verification of educational certificates using blockchain

Badhe et al. (2020) identified a problem with fake certificates in Pune, Maharashtra, India. Then the authors identified possible solutions through an extensive literature review. They found that blockchain can be a reliable solution to their problem, through the security, validity, and confidentiality it can offer.

Currently students can achieve different degree´s and education levels, due to this process a lot of certificates are produced. Then these certificates are needed when students apply to jobs in private or public institution, the verifying process of this documents can be long and strenuous, because it is done manually. Due to the nature of this process, it is possible that students manufacture fake certificates, making it hard to identify which is valid or not. These certificates can be made at a low cost. An easy access to them and the already difficult verification process make the problem harder to solve.

To solve it the authors suggest storing these files in the blockchain. After the university registers and sets up the necessary steps they can start creating immutable certificates, then these certificates are stored in Inter planetary file system (IPFS), a dedicated blockchain to store files. Then a SHA-256 hash is returned, serving as an ID for the certificate, this together with student information is stored on the blockchain. The produced transaction ID is then given to the student as a confirmation and validation tool. This can be used to check de file and the student information in IPFS.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

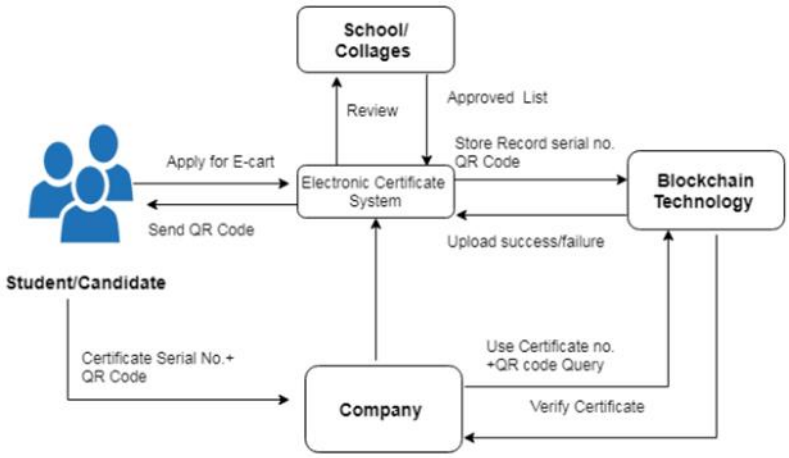

Figure 2.8. Badhe et al. *system architecture.*

Source: Badhe et al. (2020)

We can see their system in Figure 2.8. The authors conclude that automated certificate creation is transparent and open. These factors make it easy for companies to check the information given by students. The proposed system reduces costs, prevents the creation of counterfeit certificates, and gives trustworthy and precise information about digital certificates (Badhe et al., 2020).

2.2.13 Revitalizing blockchain technology potentials for smooth academic records management and verification in low-income countries.

Alnafrah & Mouselli (2021) also relied on blockchain to create a solution for counterfeit certificates but more specifically in low-income countries. For the authors the main features that made them choose blockchain are reliable information exchange, transparency, security, immutability, smart contracts, and decentralization. These features make it possible to solve some problems like data storage, authentication of student's certificates, academic records management, and credentials. Then they identify specific shortcoming of the actual system in use and how blockchain can solve it.

They start with problems related to depending on paper, or physical copies:

- The risk of tampering: physical copies are easier to forge, especially in places where records are damaged: destroyed or lost during relocating.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

- Challenges in verifying them: it is challenging to verify paper certificates manually, and it can get worse in countries that do not maintain or have a central registry of universities.
- Human resources: if the certificate is lost the process of issuing another one can get expensive and demanding of extra human resources.
- Single point of failure: if the record only exists in paper if this paper is lost or damaged the restoration of this data becomes impossible, leading to a failure of the system.

There are also problems relating to digital copies:

- Third party involvement: when digitalizing paper copies the help of a third party may be necessary. If this third party is a bad actor, it can lead to tampering of information.
- Security Breach: Even when digitalized these records are still stored in a central repository. If the central database is breached it can still lead to tampering or a damage of records.
- Exchange of records between institutions: There is no easy way to exchange information between institutions, the process requires effort, time, and human resources.

Then the authors identified five solutions using blockchain:

- Due to the decentralized and immutability features it is difficult to attack a system and change its data. If the information is changed in a node, then the other nodes will notice this change and not follow this change, only by changing it in most nodes, making it harder.
- The verifying process of certificates is also easier. The students only need to share a hash or use a private key to access their information and chose to share relevant information with companies.
- The human resources needed to maintain a blockchain network are less compared to other methods, in al the tasks that may be needed on the process.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

- A decentralized approach also solves the single point of failure problem. The information is distributed among nodes, even if a node is compromised that does not mean the whole system fails. The consensus mechanism also helps with it.
- It is possible to track changes in the network, if a bad actor decides to manipulate the information It is possible to see when it started and identify what has been changed.

After all the considerations the authors proposed system (see Figure 2.9) uses what they describe as a hybrid blockchain, a system that uses characteristics from public and private blockchains.

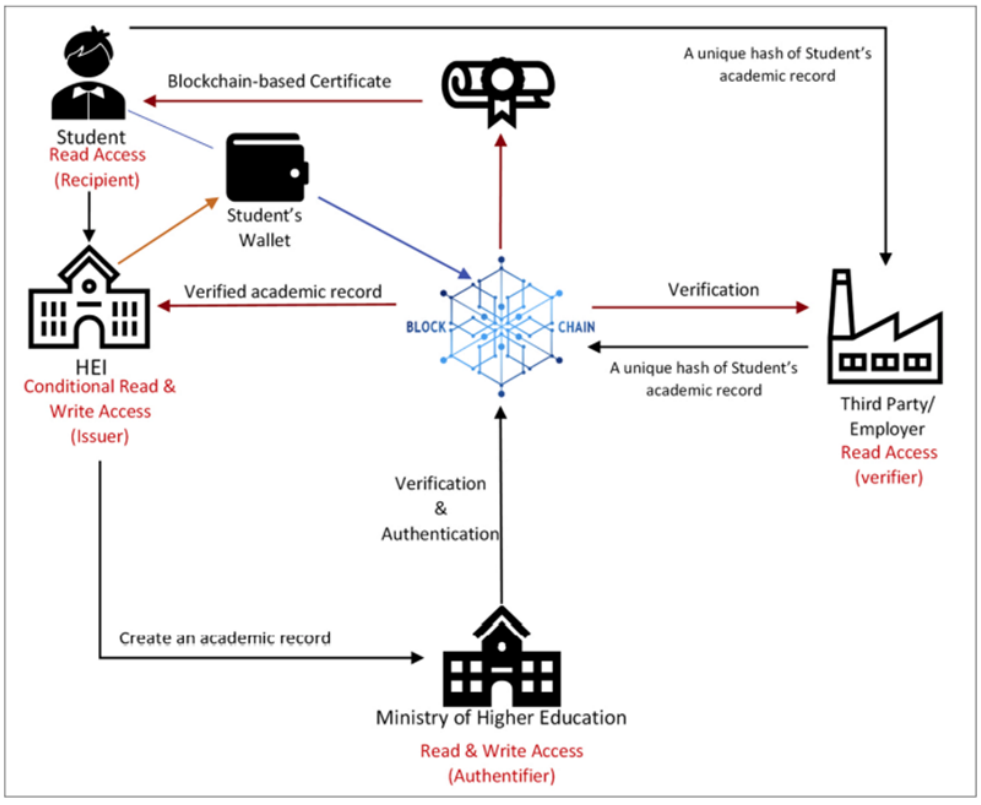

Figure 2.9. Alnafrah & Mouselli proposed system without smart contracts

Source: Alnafrah & Mouselli (2021)

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

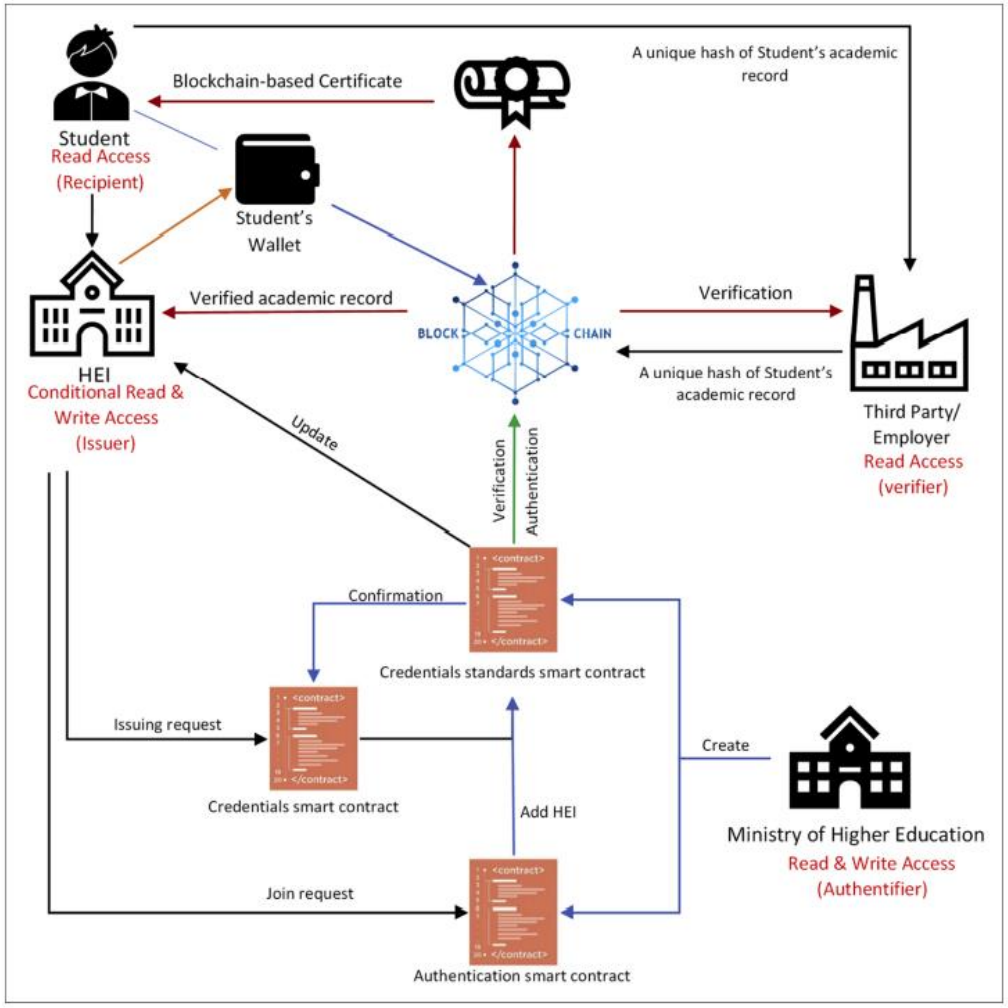

Figure 2.10. Alnafrah & Mouselli proposed system with smart contracts

Source:. Alnafrah & Mouselli (2021)

As we can see in the above figures (see Figure 2.9 and Figure 2.10) the authors propose two systems, one with smart contracts with a more complex development process and one without smart contracts, easier to implement.

Some problems relating to the implementation are also brought into discussion:

- Pre-implementation issues: blockchain can be a complex system to implement, so it's suggested that a team focused on its implementation is developed, not only in the engineering process but also in the concept and system design phases. And it's also recommended that the records are all digitalized.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

- Implementation issues: The two main factors in this stage are cooperation between the actors involved and IT infrastructure. For the system to work a well built and maintained infrastructure is needed due to the blockchain technological requirements. The relations and planning between all the involved parties must also be well developed.
- Post-Implementation: The biggest challenge would be to maintain cooperation and communication between the involved parties. To help towards it, a governance mechanism could be put in place. To create it the authors suggest using blockchain.

The deductions of the paper are that this system solves its original problem of the certificates authenticity in low-income countries. Offering a low budget and very efficient solution. Creating a national level blockchain is also the best option for all parties involved, this system can also be a vessel for better relationship with developed countries HEI's if foreign countries decide to join the system.

The paper also offers technical improvements if future works want to expand and enhance the blockchain system, for example higher transaction speed with a different consensus mechanism. The trust and credibility issue are also addressed with the use of blockchain, making cooperation between institutions and recruiters better and opening the door for a sustainable growth in low-income countries higher education. The solution is an overall good idea for the digitalization of certificates (Alnafrah & Mouselli, 2021).

Table 2.1 presents the main characteristics of the articles found in the literature review, such as year of publication, name of the authors, problem identified in the study and the proposed solution and used technologies.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Table 2.1. Papers found in the literature review

Author & year	Problem	Solution/Technologies
(Marella & Vijayan, 2020)	Verifying CV information.	Hyperledger, Frontend and SHA-256.
(Reddy et al., 2021)	Validating the credentials of graduates.	JavaScript, Truffle, Solidity, Ganache, Ethereum, and Metamask
(Sun et al., 2018)	Validating results of online education.	The specific blockchain or technologies are not stated, but a blockchain solution is suggested by the authors.
(Nguyen et al., 2020)	The use and trade of fake certificates in Vietnam.	VECefblock, with Hyperledger Fabric as a blockchain platform and deployed to Amazon EC2 service.
(Huynh et al., 2018)	Counterfeit certificates.	UniCoin blockchain, with a Full Stack application using PostgreSQL as a database.
(Alshahrani et al., 2022)	Printed certificate fraud, cost of issuing certificates and time consumed to verify issued certificates. Trust in blockchain.	Survey to test public trust on blockchain. Custom blockchain, called dApp for Smart Certificates (DASC).
(Pfefferling & Kehling, 2021)	Can blockchain be effective to use in Education Certification?	Java and RESTful APIs within the HSMW network and a separate sandbox IT-infrastructure with docker. Hyperledger and later Ethereum.
(Heredia et al., 2022)	Can we create an open source blockchain framework for education certification?	Go-Ethereum, Solidity, Web3.js and Truffle.js.
(Arenas & Fernandez, 2018)	Verifying authenticity of academic credentials.	CredenceLedger, permissioned Multichain.
(Serranito et al., 2020)	Counterfeit or falsified certificates.	Ethereum, Permissionless blockchain. JavaScript Application.
(Dumpeti & Kavuri, 2021)	Counterfeit certificates.	Hyperledger Fabric.
(Badhe et al., 2020)	Manufacture of fake certificates.	Blockchain, not stated which and IPFS to store files.
(Alnafrah & Mouselli, 2021)	Counterfeit certificates in the higher education system in low-income countries.	Hybrid blockchain.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

2.3 Discussion of the papers found in the literature review

From what we can gather in the literature review, the problem of counterfeit academic certificates is a world-wide issue. The works showed that HEI's have different levels of digitalization. Some still work only with paper copies (Reddy et al., 2021), while others have started the processes of working with digital copies, but this digitalization is still in an early stage (Pfefferling & Kehling, 2021).

The different authors identify that this focus in digitalization is a good thing. Solutions to provide a more robust system to make digital copies a more reliable means of certificates distribution are in demand. The focus of this work is using blockchain, so all the papers from the literature review use this solution to handle the digital certificates distribution and avoiding counterfeit. Blockchain is a very recent technology, but we can already see differences in its implementation.

One of these points of divergence is on the use of smart contracts. Some works end up not using smart contracts (Alnafrah & Mouselli, 2021), while other works use it (Badhe et al., 2020; Dumpeti & Kavuri, 2021). The use of smart contracts to develop applications has had an explosion on use cases recently, and it has clear advantages, since a computer defining rules and controlling these rules by itself frees up time of human resources.

Another characteristic where the authors choose differently is the type of blockchain (permissioned versus permissionless). Some researchers use permissioned blockchains (Alnafrah & Mouselli, 2021), mainly Hyperledger Fabric (Pfefferling & Kehling, 2021), an open source and highly customizable solution. The main benefits for choosing this is that the HEI controls the blockchain and does not spend money on transactions. This solution can be applied in different ways, for example, it can be a pure private blockchain, used only by one institution, or a private blockchain used by a consortium of institutions (Nguyen et al., 2020). A public blockchain can also be used, offering decentralization and transparency to the system (Arenas & Fernandez, 2018). The strong points of choosing one ends up being the weakness of the other. For instance, in a private blockchain there doesn't need to be a cost for transactions, in public blockchains there is a cost. But private blockchains end up being centralized, even if it's running on different computers there will always be a central point of control, and central systems are prone to less

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

transparency. There will also be a need to pay to maintain a private blockchain, while there is none for public blockchains. Identifying what characteristics are important for the project and choosing accordingly is very important (Alnafrah & Mouselli, 2021)(Arenas & Fernandez, 2018).

Another important decision is if the system should go full decentralized or only partial. For instance, there are solutions that offer a decentralized system to store files (Serranito et al., 2020), but an argument can be made to use a traditional database and combine it with blockchain.

Then there is the choice of technologies to interact with the blockchain and Web3. JavaScript, Python, Java or Go. The main reason to choose each can be attributed to preference, the ones the authors were more accustomed to. JavaScript offers both the frontend and the backend (Reddy et al., 2021). Python offers simplicity (Pfefferling & Kehling, 2021). Java has great support due to how long it has existed (Pfefferling & Kehling, 2021). And finally Go which is a very fast language to work with (Heredia et al., 2022). Even though the languages can be different they all end up interacting with the Web3 library (Heredia et al., 2022; Pfefferling & Kehling, 2021). The main language used for smart contracts is solidity (Reddy et al., 2021), although not much is said in the literature, there is also the option of using Rust.

All these specifications need to be adequate to the project to be efficient and make sense in the context they are applied (Alnafrah & Mouselli, 2021; Alshahrani et al., 2022).

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

3 DEVELOPMENT

This chapter presents the different stages of the software development process of EduCert, a blockchain prototype for authentication of academic degrees and certificates, namely the stages of analysis and definition of requirements, design, implementation, testing and operation and maintenance. The last two steps towards putting the software into production will not be presented because it is a prototype, which is, however, running in test mode.

3.1 Requirements

The EduCert system is composed of two main packages, as shown in Figure 3.1. 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 the users who have access to the platform, allowing the normal actions, such as authenticating them in the system, registration/deletion of users and managing their permissions.

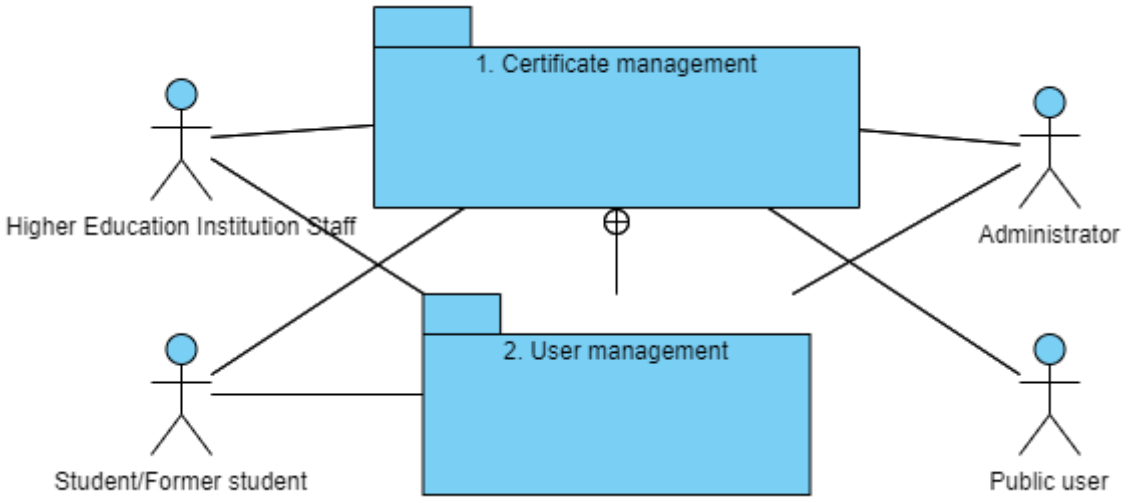

Figure 3.1. EduCert system packages.

Figure 3.2 presents the use case diagram of the certificate management package.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

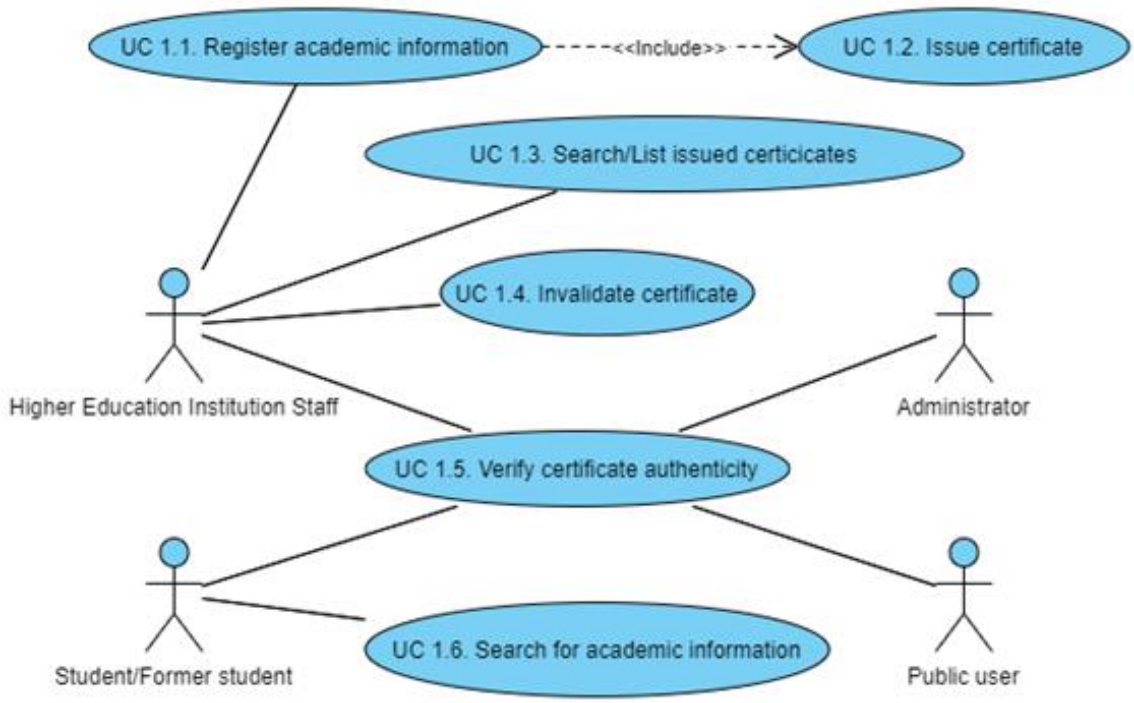

Figure 3.2.Use case diagram of Certificate management package.

The application has four types of users that can interact with the certificate (see Figure 3.2), so a management of the certificate system use cases needs to be in place. The HEI user, who manages the certificates in the system, having available the functionalities of 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. The following is a brief description of the use cases defined in the diagram (see Figure 3.2):

- UC 1.1 Register academic information – this is the first use case; it enables the HEI staff to register the academic information of specific students.
- UC 1.2 Issue certificate – this use case is related to UC 1.1, for a student to have a certificate being issued his information need to be registered.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

- UC 1.3 Search/List issued certificates – the HEI staff can then search and list all the issued certificates and the corresponding information of each student.
- UC 1.4 Invalidate certificate – This use case allows the HEI user to revoke a certificate in case there was an error when issuing the certificate. This use case will only work at the database level given the immutability characteristic of the blockchain.
- UC 1.5 Verify certificate authenticity – This use case allows users to verify the authenticity of the certificates.
- UC 1.6 Search for academic information – This use case allows registered users to search for their own information.

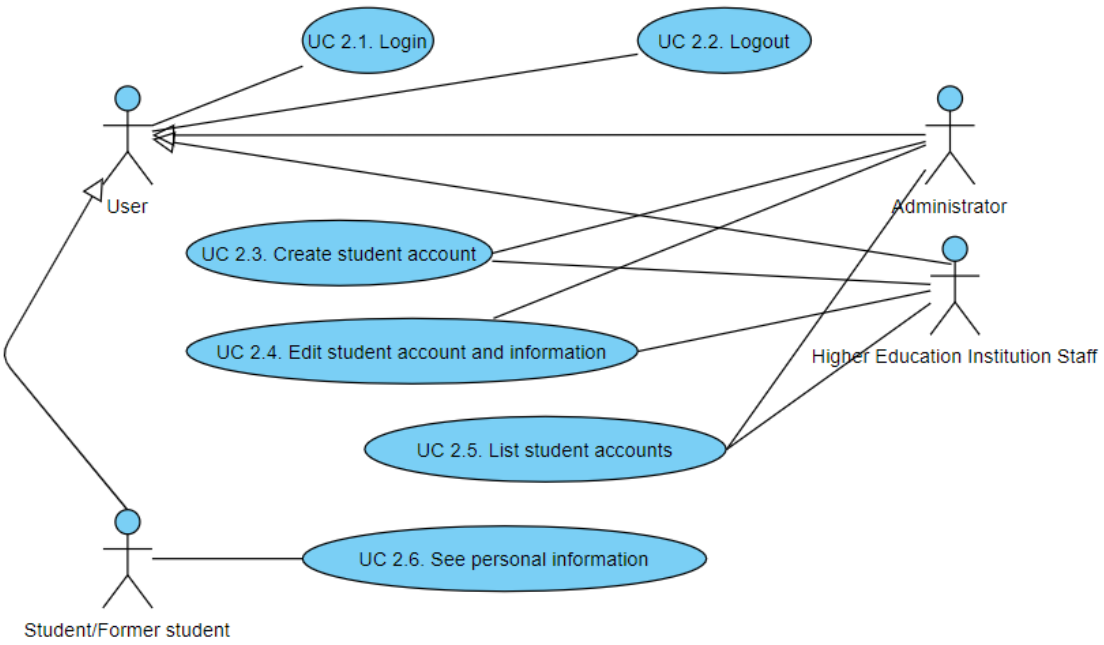

Figure 3.3. Users' management use cases.

Figure 3.3 shows the user management use cases diagram which includes typical functions such as authentication or user registration. In this diagram the "Public user" (see Figure 3.2) is not included because it does not need any type of authentication / registration in the system to be able to use it and a new type of user, called User, is included from which the others derive, called user who can perform the login and logout functionalities in the system. Then we have the students who receive an account to check

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

their information and can log in to it, to check personal information restricted to each student account. The administrator and the HEI staff, can create students accounts, list these accounts, and edit them. They can also add new information to each account referring to different students and, since they derive from User, they can also login and logout. The following is a brief description of the use cases defined in the diagram:

- UC 2.1 Login – The users can access the login screen and login if they have valid login credentials. Before logging in all users are normal users.
- UC 2.2 Logout – All the users with valid login credentials once they complete the login they can then log out of their account.
- UC 2.3 Create Student Account – The administrator or the HEI staff can create accounts for students to check their information.
- UC 2.4 Edit Student Account and information – The administrator or the HEI staff can, if needed, update or edit the information of the students in the database.
- UC 2.5 List Student Accounts - The administrator or the HEI staff can list all the student accounts in the database.
- UC 2.6 See Personal Information – Each student or former student can see their own personal information once they log in.

3.2 Design

This section presents the proposed architecture for the EduCert system and some mockups of the user interfaces of the frontend.

3.2.1 Architecture

As can be seen in Figure 3.4 the EduCert system consists of an application server, where the frontend operates and runs on the browser. The backend runs server side connecting the frontend to a database server and the block chain network. The frontend allows the different users to interact with the system to perform different operations and communicate with server-side utilities through the backend. The backend receives requests from the frontend through Hypertext Transfer Protocol (HTTP) requests to store information about students and their academic certificates both in the database and in the

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

blockchain, through a specific request, called POST. The frontend can also "ask" information to be displayed to the user, through GET requests.

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 is where the hashes relative to the certificates are stored.

The blockchain that we will use in this project is public, which can reduce some costs. The idea is that anyone wishing to verify if a certificate is valid can do so through the EduCert application. But we can't store everything on the blockchain, if the objective is to lower costs, then it becomes necessary to use a database to store more personal information that is not desired to be public in the blockchain. The information that is stored in the database can be used as a mechanism to double check the verification of the authenticity of the certificates on the blockchain.

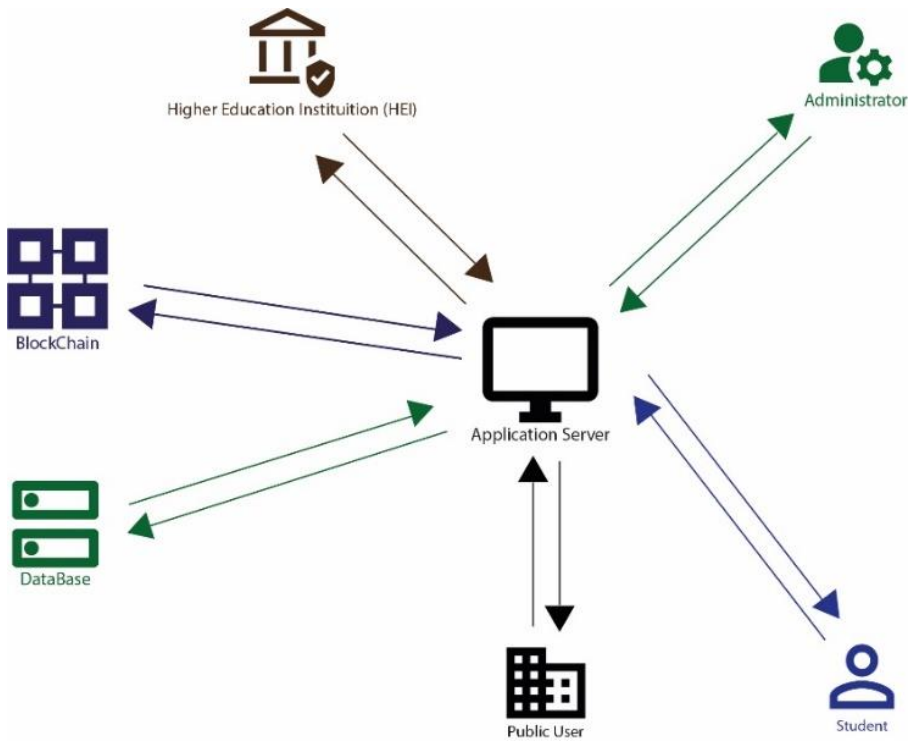

Figure 3.4. EduCert architecture.

The communication (see Figure 3.4) 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

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

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.

3.2.2 Mockups

The following images are some of the mockups of the functionalities and navigation we want to implement in the frontend application of EduCert.

One of the first functionalities to implement should be somewhere to add information. In Figure 3.5, Figure 3.6 and Figure 3.7 we can see the mockups for the Educert system to upload information. Without information there is not much we can do on our application and so this needs to be a priority screen for our system

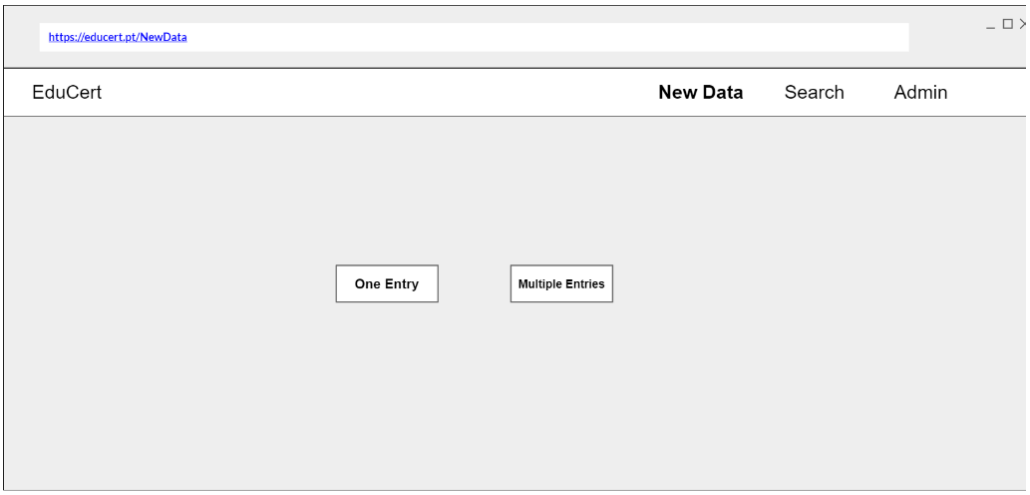

Figure 3.5. Data entry mode selection screen (UC 1.1 Register academic information).

The data entry mode selection screen is available to the HEI staff or administrators and allows them to select how the student data will be loaded. We are going to give two possibilities when uploading information to our website (see Figure 3.5), either a single entry in relation to one student or several entries in relation to several students.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

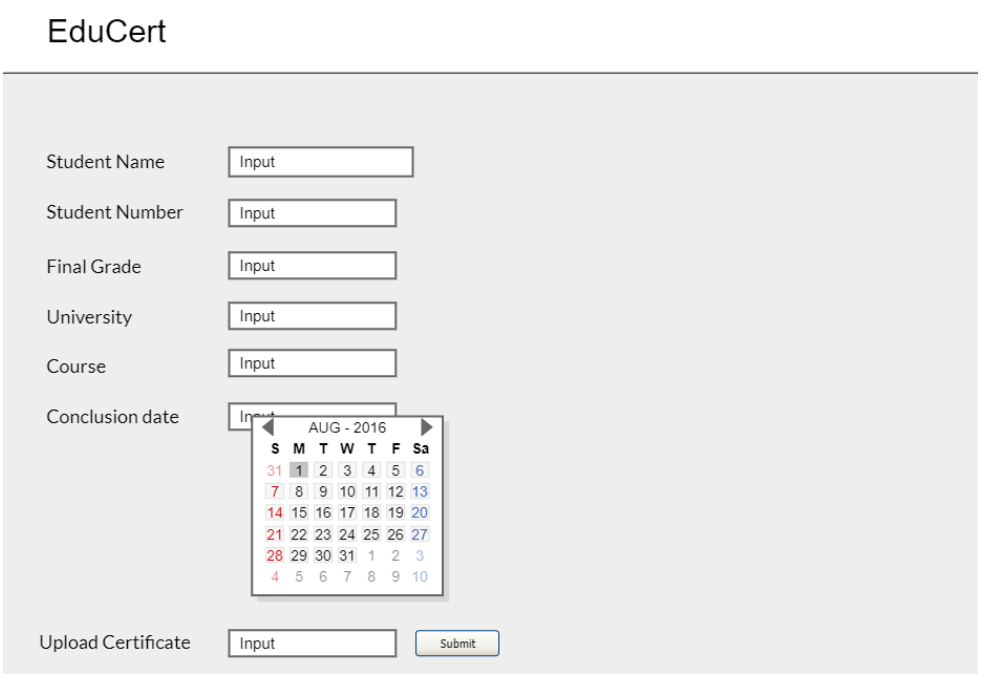

Figure 3.6. Single entry screen, to introduce data of only one student (UC 1.1 Register academic information).

Single data entry (see Figure 3.6), which is a form, that makes it possible to add information about a student at a time. It is also possible to add a pdf file to it, to link the certificate hash to the student information. For this mockup we made fields for the name, number, final grade, university, course, conclusion date and the pdf certificate. On submit the information should go the blockchain and the database server.

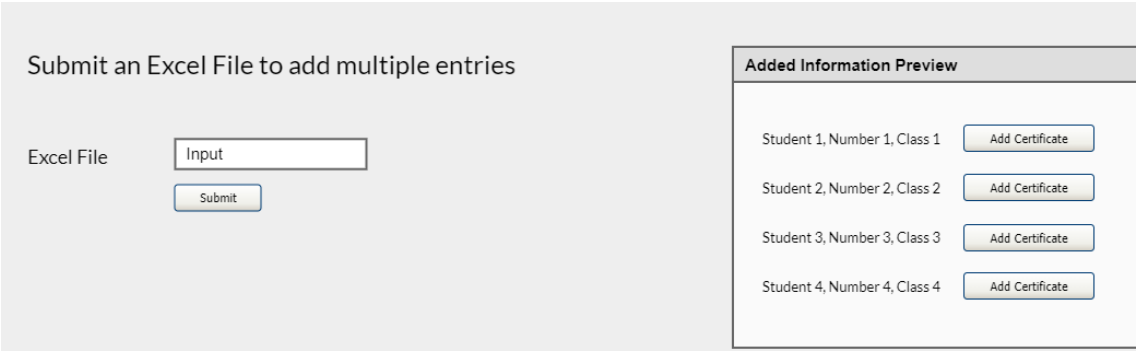

Figure 3.7. Multiple Entry Screen, to introduce multiple student information (UC 1.1 Register academic information).

It will also be possible to add information in bulk (see Figure 3.7). This will be made possible by importing an excel file. The information will then be processed and displayed on the same page, in a pop up or window inside the same page. This will show the HEI staff the information that was imported and give the possibility to add the certificate to

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

the blockchain. Then the administrator can add the certificate to the student information. The hash will be calculated through the algorithm and added to the student information.

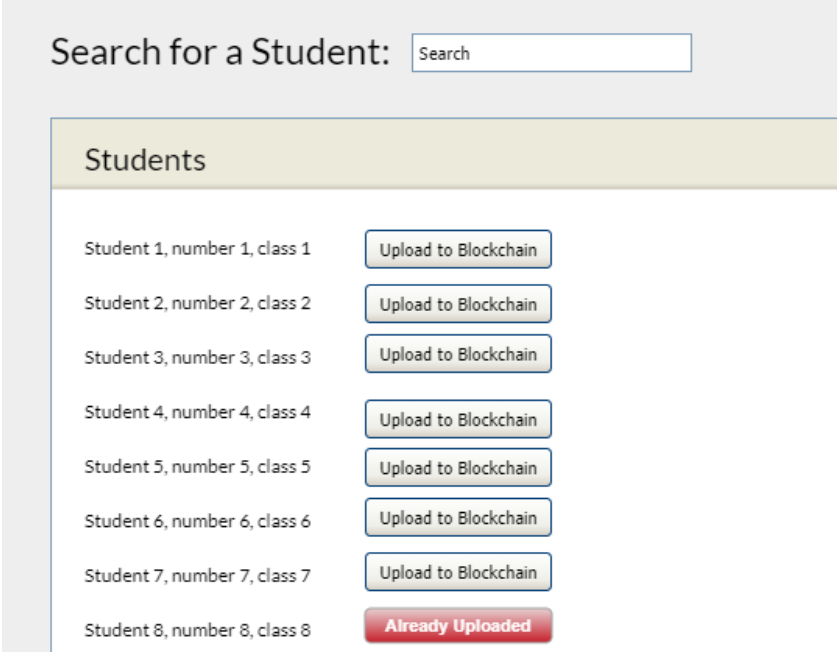

Figure 3.8. Screen where admins can see and search for student accounts/information (UC 1.3, 2.3 and 2.4).

The administrator can also search for a certain student to access or alter their data. In the screen in Figure 3.8, the administrator can also upload the hash to the blockchain and see which ones have already been uploaded, with some information about the students.

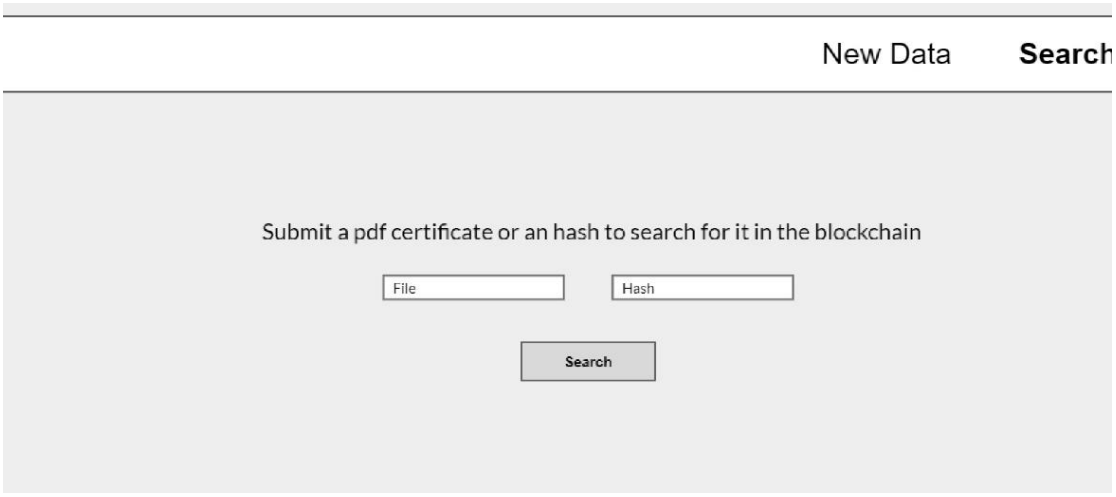

Figure 3.9. Screen to search for a Hash (UC 1.5 Verify certificate authenticity).

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

A normal user, with no login, can only search for a hash in the blockchain. He will be greeted with the screen in Figure 3.9, where it is possible to upload a certificate and search for its hash. Then the user can get two responses.

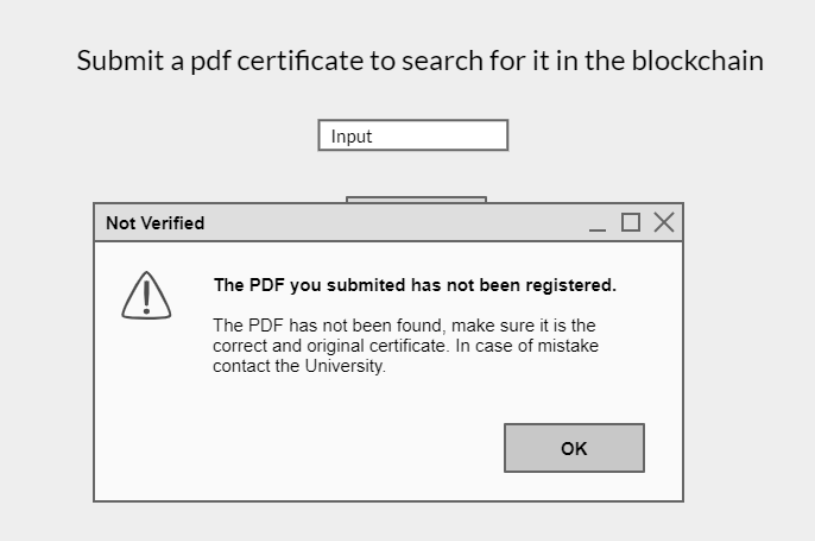

Figure 3.10. Invalid Certificate Screen (UC 1.5 Verify certificate authenticity)

One of the messages that can appear is a warning that the hash that was searched for cannot be found, if this is an error the user is advised to contact the university (see Figure 3.10).

Figure 3.11. Valid Certificate Screen (UC 1.5 Verify certificate authenticity).

The second message that could appear (see Figure 3.11) is if the user searched for a valid certificate. The user will also see in the message some information about the certificate

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

and the student that it's associated with. The information will need to be handled with care due to the data protection regulation in place.

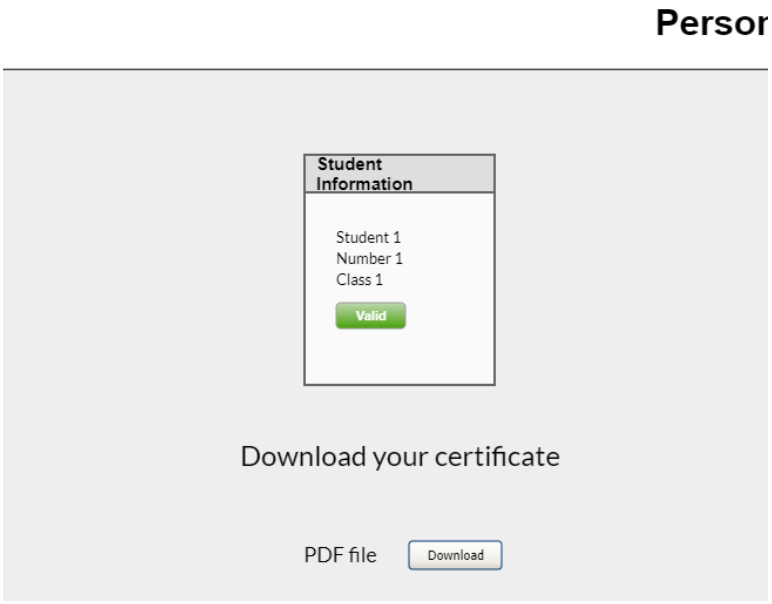

Figure 3.12. Screen where student can see personal information (UC 1.6 Search for academic information).

The student can also login to the website and see his personal information. It is also possible to download an original copy of his certificate. The user can also check the status of his certificate. If it's valid it will appear green, if it's not valid red. When the certificate is valid the user will also be notified.

Figure 3.13. Login page (UC 2.1 Login).

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Both the student and the admin need to login. So, we need a login page (see Figure 3.13). This login page will receive the username or email and the password of the user. And then will not be displayed while a user is logged on.

3.3 Used Technologies

The following technologies are going to be used to create the EduCert system:

- HTML and CSS to build each page that it's displayed, in CSS we will use Bootstrap to accelerate the development.
- JavaScript for building the frontend and communicate with the blockchain.
- NodeJS and Express for building the backend system, which communicates with the database 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.
- SQLite3 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 with 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.
- Solidity for Smart Contracts.
- MetaMask, to store Fantom tokens and connect the browser to the blockchain to pay for the publishing fees of the hash certificates.

3.4 Implementation

In this section some of the most important aspects of the coding of the EduCert system are presented and grouped by the technology used to develop them, namely, the coding of the contract that sustains the publication of the certificates on the Fantom blockchain (see Figure 3.14); the JavaScript used, for example on the hashing function for the validation on the blockchain of the PDF file (Figure 3.15), the functions for sending the hash (Figure 3.16) and the search/verification (Figure 3.17) of the certificate validity; and

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

finally, the backend with NodeJS (Nodejs, 2009) and ExpressJS (expressjs, 2010), a NodeJS framework, that helps defining routes and endpoints.

3.4.1 Solidity

In Figure 3.14, 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).

```
// 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);
    }
}
```

Figure 3.14 Smart contract (solidity).

The first function, “addDocHash”, allows adding a hash to a block. This function requires an argument, a hash, that is of the bytes32 (a string). Then we record the time, the block number and who executed this function, the message sender. This is saved in a struct that we declared earlier in the code. A struct is a data type, that stores values. These values are stored like properties of the struct. In our case we are storing the “mineTime”, the “blockNumber” and the “messageSender”, our properties, in the Record struct.

Then we use Mapping. This is a functionality of Solidity that works like a hash table or a dictionary, data types that we find in other programming languages. It stores values in a “Key: Value” pair. In our case, the key will be of type bytes32, which is our hash. And the values will be the struct, and by extension, the values inside the struct. We then name this new object, “docHashes”. Then, in the last line of “addDocHash”, we can see this

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

mapping in use. We set the key as the hash we receive and store the values as the struct we defined earlier.

The second function, named "findDocHash", searches for the hash in the blockchain returning information stored previously (if existent).

To store a hash the user needs to pay gas fees, but to search for it the user does not. This contract was then uploaded to the Fantom test-net for further use.

This contract was originally found in "Ether doc cert" GitHub repository (Dat Tran, 2022).

3.4.2 JavaScript

The JavaScript used in this project is present in diverse files, that are used like modules. Some of these modules/files were created by us, while others were open-source code in GitHub.

The first file that we used was "Main.JS". This file was adapted from a file available at the "Ether doc cert" repository (Dat Tran, 2022) that interacts directly with "NotaryWebLib.JS".

Main.JS has the hashing function. It looks for the input file and then hashes the file. This function then makes it possible for the other two functions in this file to use this hashed value. These two functions are "send" and "find". They execute the corresponding smart contract functions. Send, sends the hash to the blockchain. And find, searches for the hash. They both accept the hash as an argument. And they both return a message that is displayed as html in the page where they are executed from.

NotaryWebLib.JS is the file that is responsible for directly communicating with the blockchain. For this we have in this file the functions that connect the browser with Metamask. It also connects with the contract. For this we need to give to the function that connects with the contract, the structure, and data types that the contract will receive. This is important because we will be sending and receiving information. This is done through notary_find and notary_send. These functions execute other functions of the Web3 library

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

(ChainSafe, 2014). These two functions are used in the find and send functions of Main.JS.

The "Main.JS" and "NotaryWeblib.js" files have some dependencies, like JQuery (jQuery, 2006), a JavaScript module which offers several functionalities, the, that facilitates the communication with the blockchain through already built-in functions, and "sha256.js" (Emn178, 2017) that offers an encryption algorithm, all these libraries are open-source JavaScript libraries.

These "Main.JS" and "NotaryWeblib.js" files are responsible for the functions presented below (hashing, sending, and searching the blockchain).

```
$(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);
    }
};
```

Figure 3.15. Hashing function.

Figure 3.15, presents the hashing function that calculates the hash of the file (PDF certificate of the academic degree). To do this we use a JavaScript library that has an algorithm, in this case SHA-256 (Emn178, 2017) to calculate the hash of a document. This document is retrieved with JavaScript when the user uploads the certificate in the appropriate page. Then it will be stored on the blockchain using the "send" function presented in see Figure 3.16.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

```
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>"
            );
        });
    });
};
```

Figure 3.16. Send hash to blockchain.

Figure 3.16, shows the function used to send the hash to the Fantom blockchain. This is done using the function "addDocHash" defined in the smart contract (Figure 3.14). This is done by using a third-party module, called web3 (ChainSafe, 2014). 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 (MetaMask, 2019) 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 (ChainSafe, 2014).

```
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>"
                );
            }
        });
    });
};
```

Figure 3.17. Searching function.

The function presented in Figure 3.17, searches the Fantom blockchain for the corresponding hash, using the same principles explained for sending the hash. It starts by

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

seeing 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. The user is informed if the account that uploaded the hash is from "IPC" or not. If the hash is not on the network, the user will be notified with a different message.

```
var globalJsonObject;
$(document).ready(function(){
    $("#fileUpload").change(function(evt){
          var selectedFile = evt.target.files[0];
        var reader = new FileReader();
        reader.onload = function(event) {
            var data = event.target.result;
            var workbook = XLSX.read(data, {
                type: 'binary'
            });
            workbook.SheetNames.forEach(function(sheetName) {

                var XL_row_object = XLSX.utils.sheet_to_row_object_array(workbook.Sheets[sheetName]);
                var json_object = JSON.stringify(XL_row_object);
                globalJsonObject = XL_row_object;
                console.log(globalJsonObject);
                console.log(json_object);
                document.getElementById("jsonObject").innerHTML = json_object;


            })
        };

        reader.onerror = function(event) {
            console.error("File could not be read! Code " + event.target.error.code);
        };

        reader.readAsBinaryString(selectedFile);
    });
});
```

Figure 3.18. Excel-import.js code.

Another coded JavaScript file was "excel-import.js" (see Figure 3.18). This file was created to facilitate the import of information for the HEI staff who manage it. It reads information from an Excel file and processes it. It uses the public JavaScript library, SheetJS (SheetJS, 2014), that has built-in functions that facilitates working with Excel files. This information is then processed even further to another data type, JSON, JavaScript Object Notation, so that we can work with it on the server-side.

3.4.3 NodeJS

NodeJS (Nodejs, 2009) is an asynchronous event-driven JavaScript runtime. It makes it possible to write the backend of an application using JavaScript.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

3.4.3.1 Express

NodeJS has different packages/libraries available, that make it easier to add features to the project, using built-in functions. One of these packages is Express, it is widely used and facilitates the creation of website routes or even API's. To use express, the package needs to be required, this works like an import in other programming languages. (Figure 3.19).

```
const express = require('express');
const app =  express();
```

Figure 3.19. Instruction to import express module (Express require).

Express is a minimal web application framework. It is widely used due to its robust features to build web and mobile applications. Express offers a variety of HTTP utility functions and middleware. It offers features on top of NodeJS performance.

Express enables the creation of routes, in conjunction with http requests. Routes are the mapping of handlers functions of the application to a client request to a particular endpoint, which is a URI (or path) and a specific HTTP request method (GET, POST, and so on). The handler functions are executed when the route is matched (expressjs, 2010).

For example, a main page, which is essential when navigating a web site. Then express gives the possibility, through an anonymous function (a not named function) to pass a request and a response. These requests and responses are stored as objects. Express then gives extra functions to work with these requests and responses. Enabling us to for example in response to a get request render a page. Or send an error message to the browser, and then the browser displays an error page. We can also write normal JavaScript logic inside these routes.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

```
app.get("/logout", (req,res) => {
    user = null;
    res.redirect("/");
});

app.get("/", (req,res) => {
    res.render("index.ejs", {students, user});
});

app.get("/new-data", (req,res) => {
    res.render("newData.ejs", {user});
});

app.get("/search", (req,res) => {
    res.render("search.ejs", {user});
});

app.get("/login", (req,res) => {
    res.render("login.ejs", {user});
});

app.post("/login", (req, res) =>{
    const {username, password} = req.body;
    if (username === "admin" && password === "admin") {
        user = "admin";
        res.redirect("/");
    } else {
        res.redirect("/login");
        console.log("Not a valid User")
        user = null
    }

});

app.get("/new-data/one-entry", (req,res) => {
    if (user === "admin"){
        res.render("aluno.ejs", {user});}
    else {
        console.log("Not a valid user")
        res.status(401).end()
    }
});

app.post("/student", (req,res) => {
    const { name, num_student, class_final, Institution, Course, conc_date, certificate } = req.body;
    students.push({name, num_student, class_final, Institution, Course, conc_date, certificate});
    res.redirect("/");
});
```

Figure 3.20.Routes created for the application

Different routes were created to help develop the app in the initial stages to make some tests. Then we developed the final routes after having a better understanding (see Figure 3.20). It is also possible to define the type of request for each route. There are various types of requests, but two specific ones used here. We can have a GET request, that requests information to be displayed to the user. And a POST request, where a user can send information to the server.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

In this case the POST request was used to send the student information to be stored, with the route "/student". Then this request is destructed, which is the JavaScript way to remove certain parts of an object. This is needed because there can be bad actors who find a way to send more information than the one which is required.

We can also do a GET requests. There are the most common, as most of the time we are displaying information for the user. It is then possible to write code inside this request. Normally we render a page, as we can see on the second route, "app.get ("/"), but we can also do other things. For example, in the "/new-data/one-entry" we write some logic on the request. So that it behaves differently depending on who is the user.

3.4.3.2 EJS package

Another important package is Embedded JavaScript templating (EJS) (see Figure 3.21), which allows HTML file templates to be created, with json data loading from variables stored on the server side or databases making web applications dynamic. In Figure 3.22 is possible to see a for loop that loads the name and certificate from the database.

```
app.set('view engine', 'ejs');
```

Figure 3.21. EJS package.

```
<body>
    <h1>Comments</h1>
    <ul>
        <% for(let st of students) {%>
        <li>
            <%=st.name%> - <b><%=st.certificate%> </b>
        </li>
        <% }%>
    </ul>
    <%= console.log(students) %>
    <a href="/student">New student</a>
```

Figure 3.22. For loop with EJS.

3.4.3.3 Login system and permissions

Another important part done in Node, is the login system. We can see in the routes image (see Figure 3.20), that we have two "/login" and a "/logout" route. The POST "/login"

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

route retrieves the username and the password that the user wrote on the page and passes this information to our server. This is done through server-side variables to store the information. To start we made only an admin account. And then we check if the username and password are the correct ones for the admin account. If they are, we will set a global variable that we defined earlier, called user, to admin. The function of this variable is to control who is the user that is logged in is. And finally, we redirect the user to the main page. If the username or password are not the ones we define for the admin account, we will redirect the user to the login page again, inform the server through a console log that the user is not a valid one and set the user to null.

The GET request for "/login" is only used to render the information to the login page. The get for "/logout" is written but is not meant to be accessed normally, it will be used only when the user presses a button. This will change the value of user to null and redirect the user to the main page.

Combining the EJS templates, with the login system we implemented, we can make pages display information depending on who the user logged in is. One example of this can be seen in Figure 3.23. We make a navbar that only shows certain pages depending on who the user is, in this case if the user variable is set to admin.

```
<% if (user === "admin") { %>
    <nav class="navbar navbar-dark navbar-expand-lg navbar-color">
        <div class="container-fluid">
            <a class="navbar-brand" href="/">EduCert</a>
              <div class="nav text-color-white">
```

Figure 3.23. EJS login System.

Even though we can control what the user sees, if a user that is not the admin knows of the existence of an admin only page, s/he can try to access it. To prevent this, we also program some logic to certain routes. Returning to Figure 3.20, in the GET route, "/new-data/one-entry", where the admin can insert student information, we can see an example of this logic. If the user is the admin, we will render the page, if he isn't we will display the status code 401, which means unauthorized user. This solution for a login system works as an example or a prototype but is not advised for applications in a production state.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

3.4.4 SQLite3

Having in mind the scope of this project we decided to use SQLite3 as a database. To use it in EduCert system we need to create a Javascript file called "Database.JS". This file gives instructions to the server on how it should interact the SQLite3 database, allowing one to transmit SQL statements, such as creating tables (Figure 3.24).

```
const sqlite3 = require('sqlite3').verbose();

const DBSOURCE = "db.sqlite"

let db = new sqlite3.Database(DBSOURCE, (err) => {
    if (err) {
      // Cannot open database
      console.error(err.message)
      throw err
    }else{
        console.log('Connected to the SQLite database.')
        db.run(`CREATE TABLE user (
            id INTEGER PRIMARY KEY AUTOINCREMENT,
            name text,
            student_number text,
            final_class number,
            institution text,
            course text,
            conc_date date,
            certificate_hash text,
            on_blockchain text,
            email text ,
            password text
            )`,
```

Figure 3.24. Part 1: Database creation code.

In Figure 3.24 we can see how the "Database.js" works. It creates a template for the database to use. In here we define the name of the table. That we named "user". In here we chose to have a unique identifier or id, the name, number, final grade, institution, course, conclusion date, certificate hash, email, and password, all this information is regarding students or even administrators. Then we also have a "on blockhain" field that will be used to verify if the hashes were sent to blockchain.

Then, after we pass the template, we create the table by using an if statement. We need this if statement because the database creation file always run when the server starts. We control this state through an error variable. This if statement purpose is to verify if the database file exists, it uses the error variable to verify the state of the database. If it already exists, the database will not be created again. If there is no error the database is created from the start. On creating the database, we create some dummy data with it.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

3.5 Functional testing

We developed some functionals tests to validate the EduCert system prototype against the functional requirements/specifications defined in section 3.1.

Although all the functionalities were tested, in this section we only present the most relevant which are the registration and issuing of certificates and their validation. In the following chapter, in which the application usage flows are presented, it is possible to see other functionalities of the application.

3.5.1 Register academic information

The process of registering information was divided into two parts. The single data entry and multiple data entry.

3.5.1.1 Single data entry

To test this type of data entry we filled the form page with dummy data. Then we submitted this information and saw in the server console if the server was receiving the information sent. The POST request went through, and the information was parsed correctly from the request body to our SQLite database. Then we checked if the information could be displayed correctly, and it was.

3.5.1.2 Multiple data entry

Then we tested the capabilities of the bulk import or excel import (see Figure 3.18). We made an excel file with dummy data (see Figure 3.25) and submitted it to the page. The file was well processed, and the information was displayed correctly. We had a page that displayed the information on our database, in this page the information was correctly appearing.

name	num_student	Institution	Course	certificate
Manuel	12345	Iscac	MCTES	
Teresa	12346	Iscac	MCTES	
Jose	23456	Iscac	MCTES	
Pedro	33444	Iscac	MCTES	
Maria	12347	Iscac	MCTES	

Figure 3.25. Excel example, with dummy data.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

3.5.2 Validate certificate authenticity

We decided to isolate the certificate submission and searching of the certificate in the blockchain. We created a test pdf (see Figure 3.26) and went through the process.

Figure 3.26. Pdf used for testing

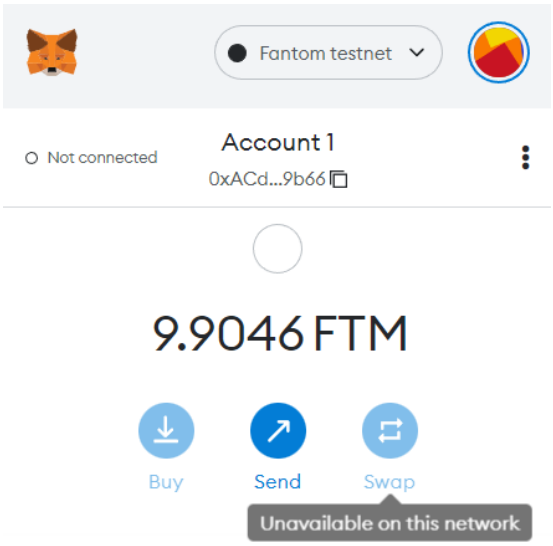

Figure 3.27. Metamask account

We tested one of the main functionalities, hashing of the document and sending it to the blockchain (see Figure 3.15 and Figure 3.16). To do this we had to setup different things. First, we created a test pdf file (see Figure 3.26) and submit it. Then we setup a Metamask account (see Figure 3.27), so that we could process the transaction, and gave it fake

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

phantom currency, this is done through a "faucet", a mechanism that gives testing currency to developers. When we had everything set up, we submitted the file for hashing, and sent it to the blockchain. Everything worked correctly.

Then we search for it, before, and after submitting it to the blockchain (see Figure 3.17). When the pdf wasn´t in the blockchain, the page gave the information that the file did not exist. If the pdf file was on the blockchain (after submitting it), the page would inform you that the pdf existed

Then we made a slight change to the pdf, only pixels, to see if the hash was the same. Even the slightest change makes the hash different. So, we need to always have an official version of the pdf for it to work correctly.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

4 DEMONSTRATION

In this section the EduCert system is presented with screenshots of the prototype, a website developed in localhost, through the presentation it is also possible to see how the application could be used by a normal user and an admin.

4.1 Landing page

We started by developing the landing page and the navigation (see Figure 4.1). The landing page has an action button that takes the user to the search page, this is called a hero section, which normally has a call to action, in our case, a button. It is also possible to use the navigation bar.

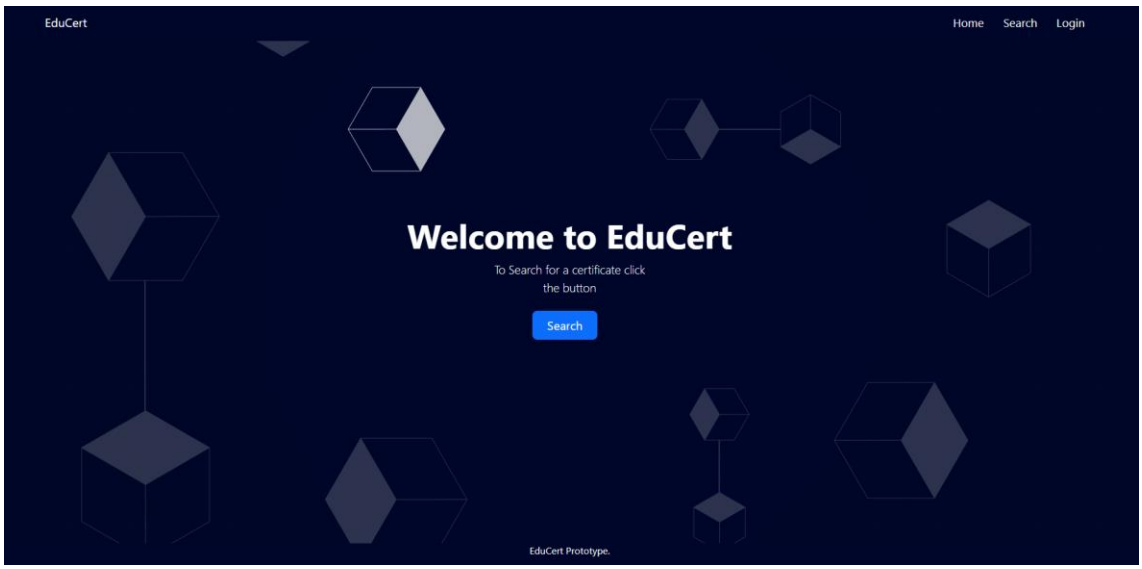

Figure 4.1. Landing page of EduCert.

Through the navigation bar we can go to the search page or to the login page. If we go to any of these pages, we can return to the homepage using the Home link. We also designed the background image and used it in some of the pages. If a user logs in, the "Login" text will be replaced by the user, as we will see later. As soon as the user joins the website, if s/he has the metamask extension, the extension will automatically try to connect to the site (see Figure 4.2).

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

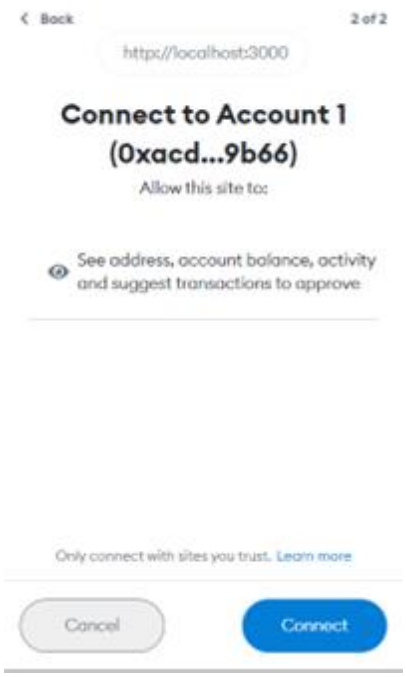

Figure 4.2. MetaMask use: connect to site.

4.2 Validating/Searching a certificate

Figure 4.3 shows the search function (see Figure 3.17) page.

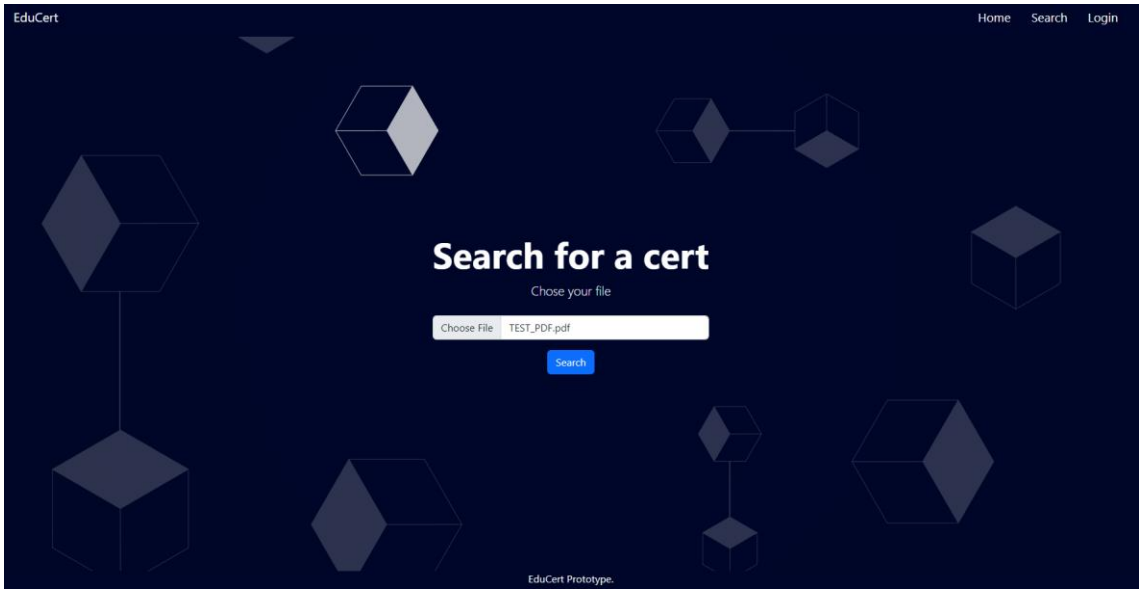

Figure 4.3. Search page.

As we referred before, if a user is logged in the information will be displayed in the navigation bar, where "Login" is written, so right now we are seeing the page as a user

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

that only accesses the page without login. This search function is the main functionality that a normal user could access. It is possible to submit a pdf file and search for it.

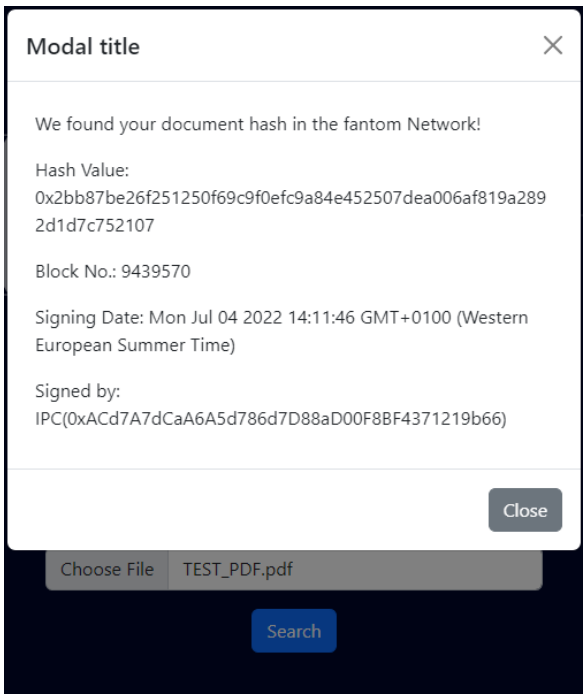

Figure 4.4. Search function modal.

After the file is submitted and the user presses the search button the information will be processes and displayed in a modal popup window (see Figure 4.4), that will show information regarding the file, like the HEI (in this case Polytechnic of Coimbra) who signed the certificate. If the file in not found a different text will appear.

4.3 Login

One of the pages that a user can access is the login page (see Figure 4.5). He will only be able to proceed further in this page if he has some credentials to login. For presentation purposes we used an admin account. We will procced by logging in and seeing some functionalities (see Figure 4.6).

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

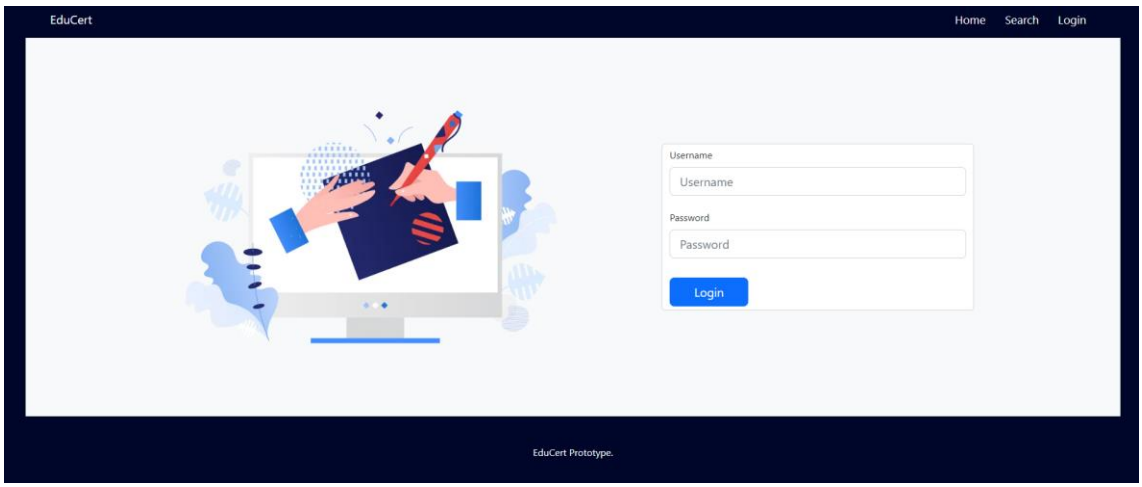

Figure 4.5. Login Page.

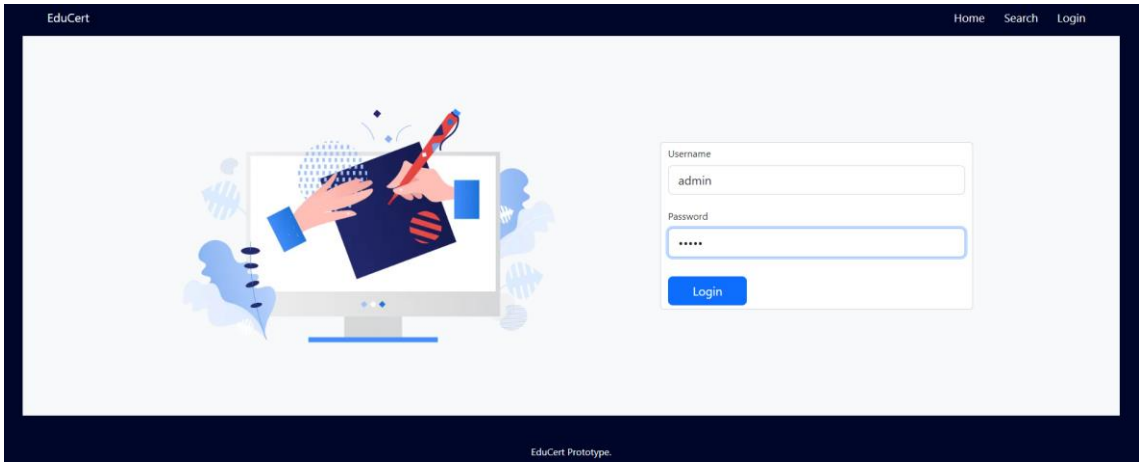

Figure 4.6. Login page - admin credentials.

In Figure 4.7 we can see the home page of the Admin user. The user is redirected to his new home page after the login, this page doesn't differ much from the non Admin user login page (see Figure 4.1), except that in the navigation bar, in the top right corner, the Admin user can access more pages of the website, only available for him, and the log in page is replaced by an indication of the account we are in and a log out dropdown button (see Figure 4.8). When the Admin user clicks on it, he is returned to the normal home page (see Figure 4.1).

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

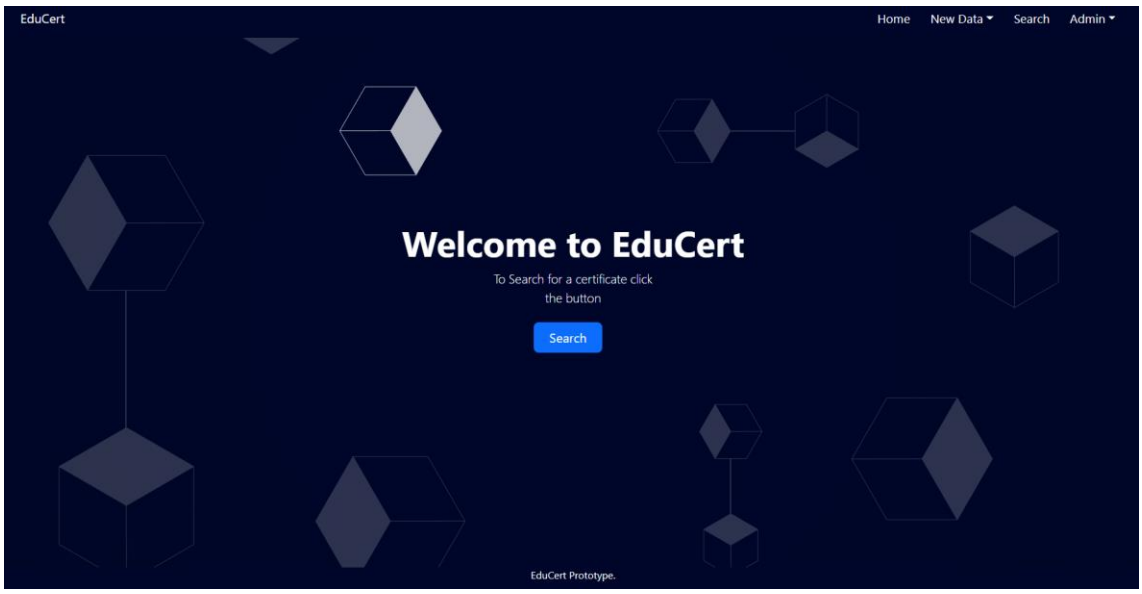

Figure 4.7. Admin user home page.

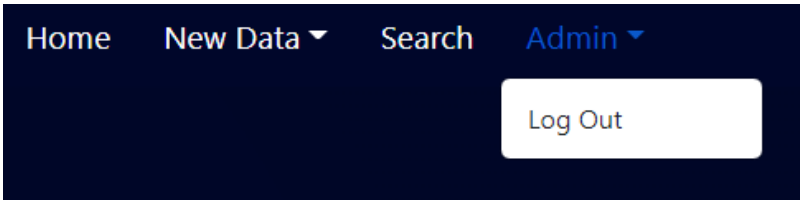

Figure 4.8. Log out button.

4.4 Adding student information

Adding student information and issuing certificates can be done by two types of users, HEI staff or the Admin user. After logging in (see section 4.3) these users can click the "New Data" tab in the navigation bar and choose one of the two options available: one and multiple entry, two separate pages. Instead of having a page with two buttons, like the mockup (see Figure 3.5), the pages can be accessed through a dropdown menu (Figure 4.9). It contributes to a cleaner design and a more lightweight website.

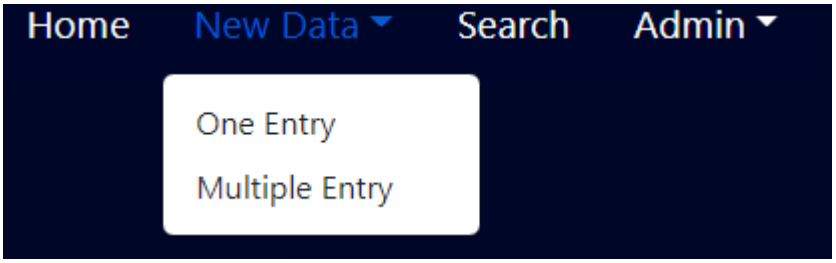

Figure 4.9. One or multiple entry dropdown.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

4.4.1 One entry

Starting by the "One Entry" page (see Figure 4.10), the user can fill a form with information regarding the student and upload a certificate, then he can submit this information for the database and send the hash of the certificate of the student for the blockchain.

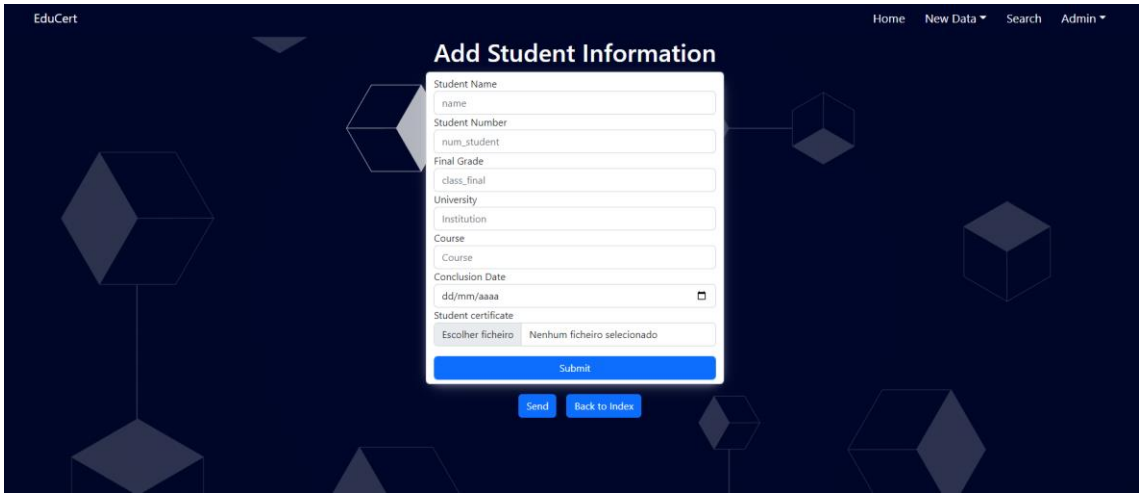

Figure 4.10. One entry page.

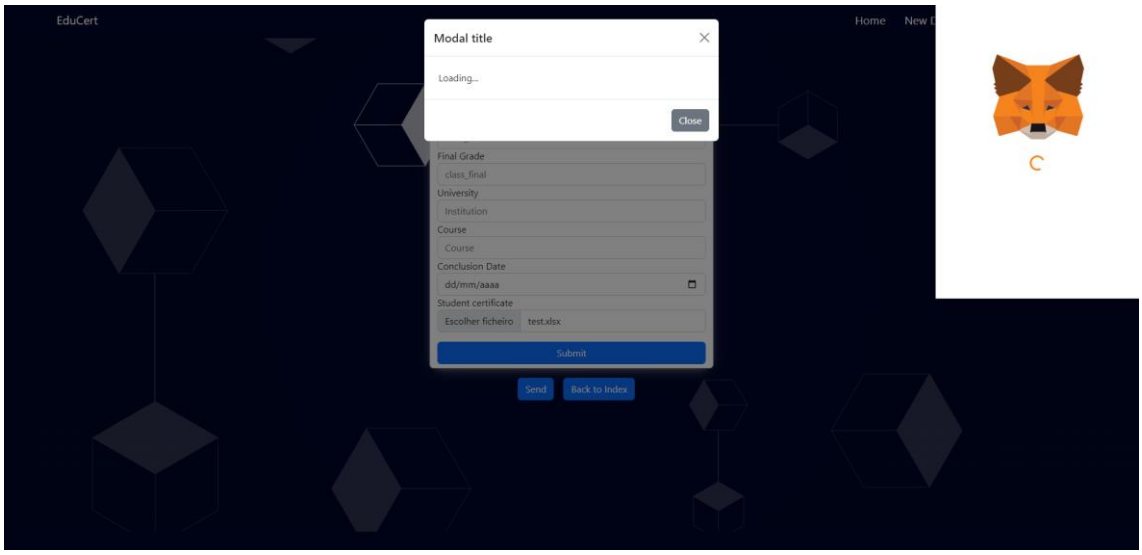

Figure 4.11. Hash sending loading page.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

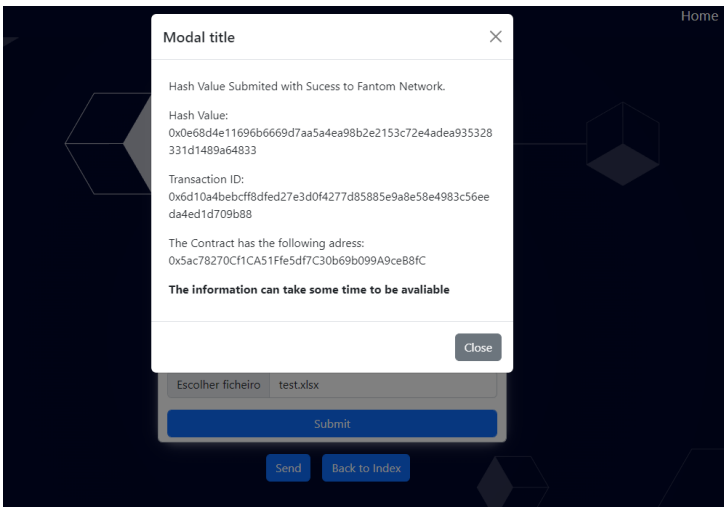

Figure 4.12. One entry - Modal with the sent information.

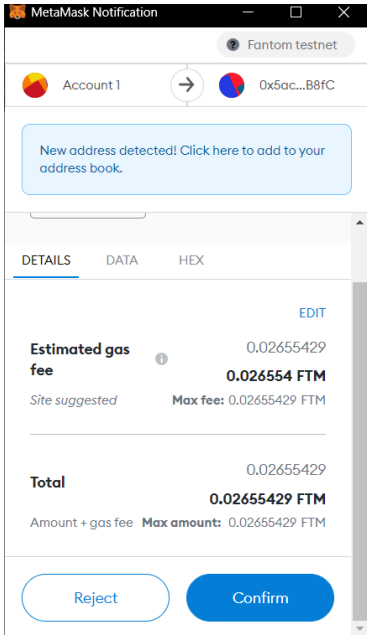

Figure 4.13. MetaMask use: confirm transaction.

When the user presses the send button, the modal popup with the information and the metamask account will start loading (see Figure 4.11 and Figure 4.13). After the transaction is confirmed, the loading text in modal popup will change to the information of the transaction. Because we are testing in a Fantom testnet there is no delay in the time the certificate is sent and the information is receiver, but if the main net is used there could be some delay to the process. So, we wrote an appropriate message if this happens.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

4.4.2 Multiple entry

The bulk or multiple entry page (see Figure 4.14) works in a different manner. Instead of having a form, that someone can fill, this page offers an input field that supports excels files and translates this information to a JSON object, a type of data that can be understood by NodeJS (Nodejs, 2009 through JavaScript, and later stored in a database. This Excel file needs to follow a certain format as seen in Figure 3.25. Then, if the user wants to see a preview of the data, we added a button, "See Data Preview", that shows the information (see Figure 4.15) in a modal, as seen before. This information is displayed in the JSON object, in a "Key:Value" format. Then the admin can submit this information. This information is sent through a POST request, that is defined in a route, in Figure 3.20, the route "/students".

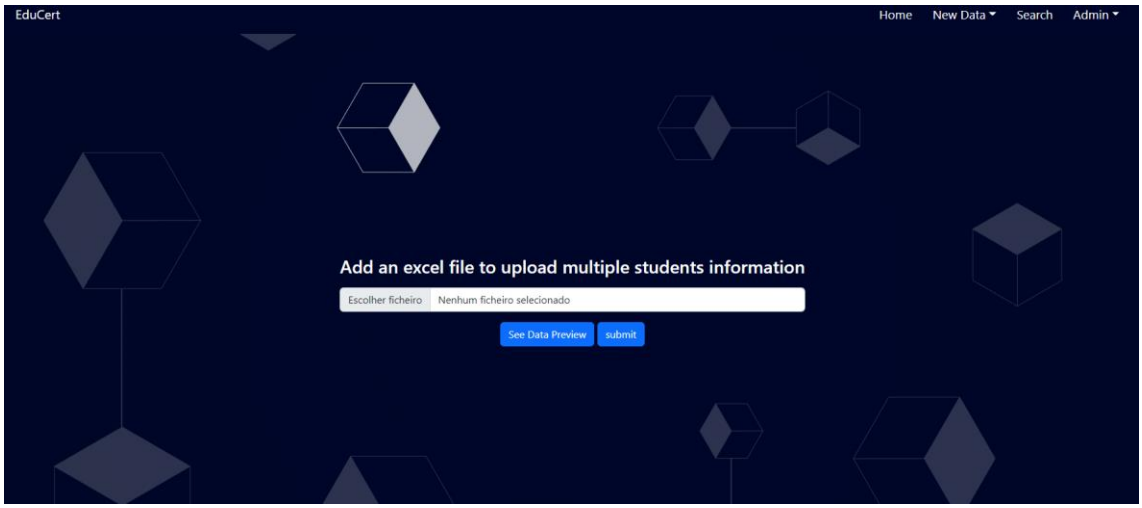

Figure 4.14. Multiple entry page.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

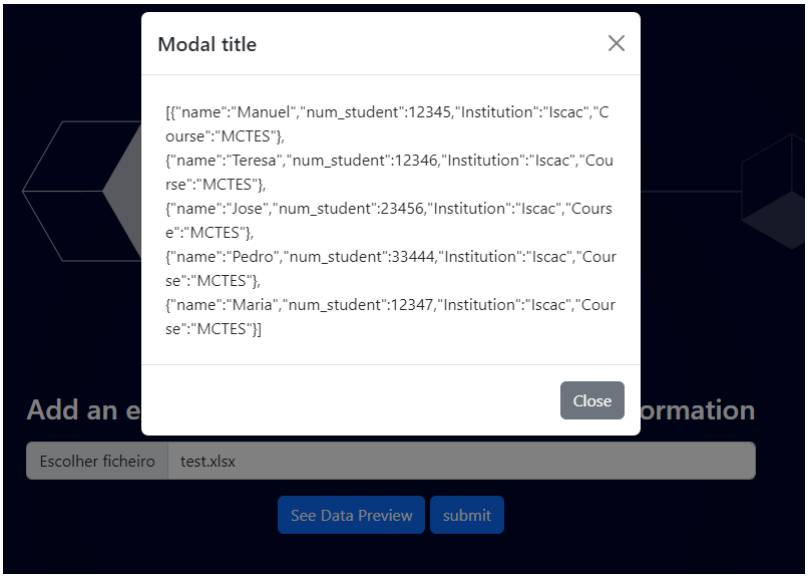

Figure 4.15. Multiple entry - Modal with the sent information.

4.5 Database

The data that is processed in sqlite3 is then showed in the page (Figure 4.16) with the help of ejs (Figure 3.21). This is done through conditions and other JavaScript functions. One of these examples is the blue buttons we can see. If the certificate hash wasn't added to the rest of the information the admin or HEI staff can add it later. The same if the hash wasn't sent to the blockchain. In this page we can add this information to the blockchain. This page also works to see the overall information about students and other staff.

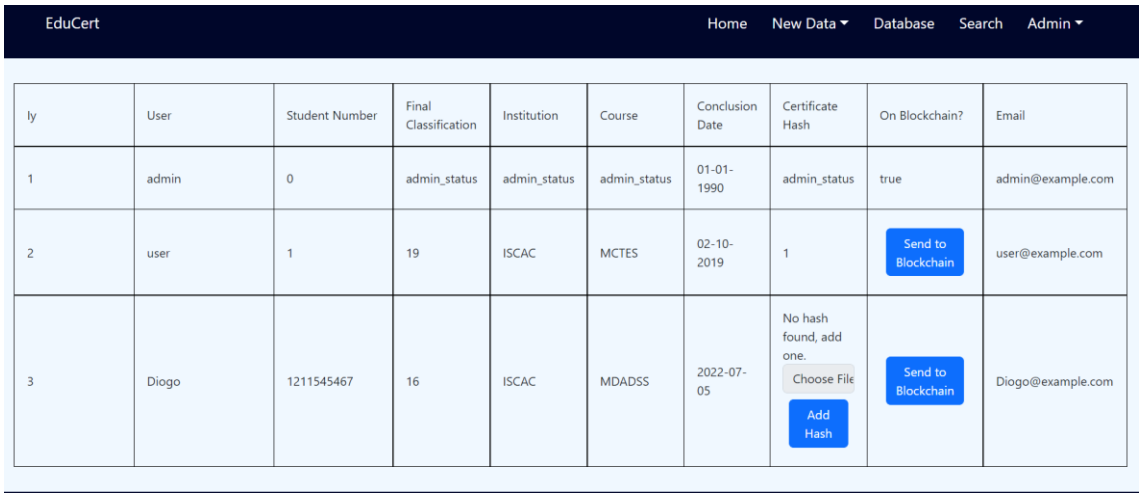

Figure 4.16. Database Page.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

4.6 Certificate

A certificate model (see Figure 4.17) would help to standardize the certificates that are given to students. Making it easier to generate and handle. We haven't made an automatic certificate generator. The certificate creation is manual. But if we transform the fields of the certificate into information receivers, we can generate new certificate with the student information.

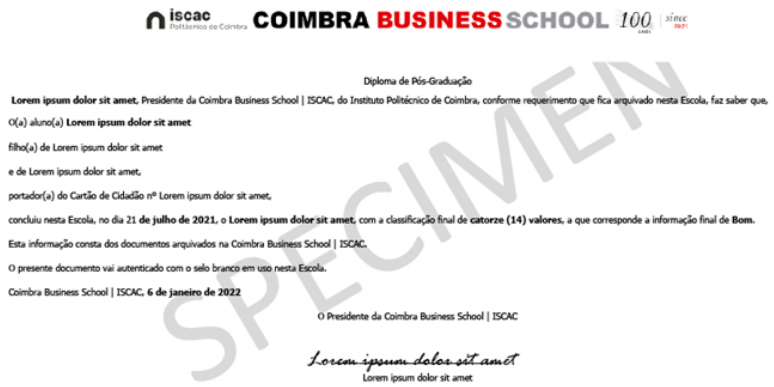

Figure 4.17. Specimen PDF certificate.

A good functionality addition, especially in a world that is more dependent on digital, would be a QR code (see Figure 4.18) on the certificate that automatically searches for the hash of itself. Making the work of the HR teams easier and more comfortable. This ease of use could give the app more users.

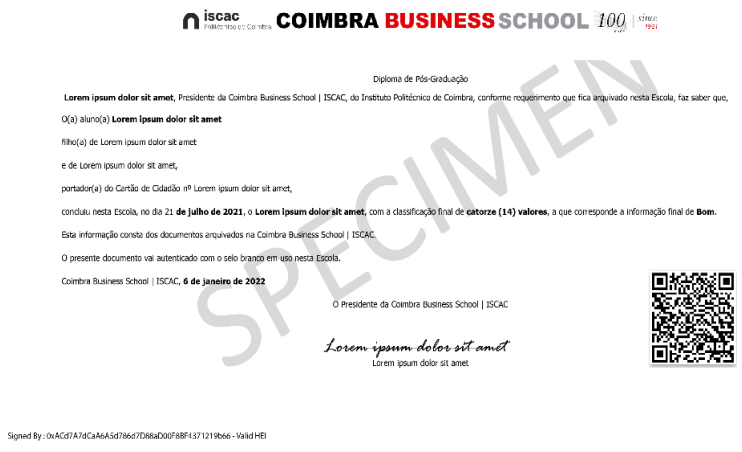

Figure 4.18. PDF certificate with QR Code and HEI signature

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

5 CONCLUSION

In this section we will talk about the conclusions about our work. We will begin by presenting a summary of the development of EduCert, then some of the contributions and what we accomplished with this work. Lastly, the limitations of EduCert and what can be done in future works to improve it.

5.1 Work Summary

This project presents the prototype developed for the validation of academic degree certificates, the EduCert.

We started by researching blockchain, to have a deeper knowledge in how blockchain systems work and latter similar works, to know how blockchain could be applied in HEI to verify certificates.

Then we thought how the requirements, like the use cases, and the architecture of the system should be. Then we developed some mockups to have an idea of the final product. After this we chose the technologies based on the literature we read and what we knew how to use, to facilitate the development. In the implementation we went through the code that was written for each technology used and tested the developed code.

In the development phase, we made 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 backend component that records information in the database and in the Fantom blockchain (the certificates' hashes). Then we presented what we made. In the testing phase, the system proved to be functional, being now necessary to test it in a real context.

5.2 Contributions

A project of this nature gives the opportunity to develop technical skills and a deeper knowledge of new technologies and new fields. Deep research makes the practical component easier to apply. This made it easier to improve on knowledge already possessed by the student, like JavaScript and NodeJS (Nodejs, 2009) and develop new ones like Solidity. There was also the opportunity to put in practice knowledge learned in

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

the master's degree, as working with more usual SQL based databases and a new kind of databases, blockchain, also the manipulation and transformation of data.

Of the various contributions of this work, the research made into various kinds of related works could be useful to develop unique and custom solutions. The application that was created also gives other investigators a framework where they could build and develop their own solutions. With a backend, a simple frontend and the connection with the blockchain there is already a good foundation to work upon.

5.3 Limitations

When we think about limitations a summary of the costs per certificate to have such a system are important to think about. In the case of Fantom blockchain, chosen for this stage of the system, the costs are about 0.026 FTM (0.01 euros), as you can see on Figure 4.13, while if chosen the Ethereum network are around 0.12 euros. The Ethereum network may be the option for the final system because it gives more guarantees of future, 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 that will lower transaction prices (gas fees costs) which will make the system even cheaper. Even though Ethereum is a better bet than Fantom for the future, it is still doubt if the technology will last. Cryptocurrencies projects can disappear during Bear markets due to people preferring less risky assets. And if a project disappears the blockchains associated with them will also disappear. Now this brings into account if a self-maintained blockchain (private) is better, using Hyperledger for example. But the costs of maintaining this kind of systems can be a limiting factor.

The use of Metamask (MetaMask, 2019) is also a limitation. Metamask is used to communicate directly with the blockchain. It is used to upload a hash to the blockchain and to make the connection when searching for a hash. Despite this making the development experience easier, it makes the project dependent on it. In turn, this can make people stray away from using the app due to having to install a third-party chrome extension.

The time constraints are also a limiting factor. Developing software is already a slow process with multiple stages, coupling this with the time spent researching make it

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

difficult to produce a final product up to standards of the current market. Nonetheless a high-fidelity prototype was achieved.

5.4 Future Works

Having into account 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.

Some suggestions, for the academia, are the use of a Non-Fungible Token system, another solution for solving an ownership problem with blockchain. Another interesting approach could also be the development of a costume blockchain and use this in the entire education system in Portugal, bringing innovation and digitalization.

Relating to our work in particular, the system still needs some changes to be up for production. One of this is the use of a better login system. The one we use is something more proper for a testing environment. But there are already some solutions for production in NodeJS (Nodejs, 2009), some very good tools for this could be “Auth0 “or “Passport”, that are reliable modules, used by different top companies.

Another change would be to the smart contract. A function in the smart contract that enables the deletion of a hash would be a good addition, we can see an example of this in another Portuguese work Serranito et al. (2020). In their work they use a deletion function to invalidate certain certificates. They also make their work available for the community, so good ideas from their work could be implemented.

Heredia et al. (2022) use an interesting approach that could solve some of our problems. For example, instead of metamask, that is a fully developed application that works as a client to work with the blockchain, they use Go Ethereum, which works the same way, but it’s fully programable, instead of a third-party client the blockchain interaction mechanism could be done all in our application. Go is an extremely useful language. Our frontend uses JavaScript, in this regard there’s not much we can do, but our back end also uses JavaScript, through NodeJS, this is not bad, but if our app grows the slow speed of NodeJS would be noticeable. Go could also be used as a backend, as a server for our JavaScript to run. Go is an extremely fast language, comparable to C. It is also statically

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

typed, the data types of each variable need to be declared once and will not change. Contrary to JavaScript, which is dynamically typed. Statically typed languages give type security to our application. If someone inputs the wrong type of data without this type of security, it can easily cause errors. All these factors make Go an interesting choice for a backend and a blockchain client.

In the department of the certificates, creating a tool to automatically create the certificates and then appending the QR code can also be a time saver and a great addition.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

REFERENCES

Alnafrah, I., & Mouselli, S. (2021). Revitalizing blockchain technology potentials for smooth academic records management and verification in low-income countries. *International Journal of Educational Development*, *85*. https://doi.org/10.1016/j.ijedudev.2021.102460

Alshahrani, M., Beloff, N., & White, M. (2022). Towards a Blockchain-based Smart Certification System for Higher Education: An Empirical Study. *International Journal of Computing and Digital Systems*, *11*(1), 553–571. https://doi.org/10.12785/ijcds/110145

Arenas, R., & Fernandez, P. (2018, August 13). CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials. *2018 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2018 - Proceedings*. https://doi.org/10.1109/ICE.2018.8436324

Badhe, V., Nhavale, P., Todkar, S., Shinde, P., & Kolhar, K. (2020). Digital Certificate System for Verification of Educational Certificates using Blockchain. *International Journal of Scientific Research in Science and Technology*, 45–50. https://doi.org/10.32628/ijsrst20758

Buterin, V. (2013). *A next generation smart contract & decentralized application platform*. https://translatewhitepaper.com/wp-content/uploads/2021/04/EthereumOrijinal-ETH-English.pdf

ChainSafe. (2014, November 5). *Web3.js*. Git Hub. https://github.com/ChainSafe/web3.js

Dannen, C. (2017). *Introducing Ethereum and Solidity*. Apress. https://doi.org/10.1007/978-1-4842-2535-6

Dat Tran. (2022). *Ether doc cert*. GitHub. https://github.com/datts68/ether-doc-cert

Dumpeti, N. K., & Kavuri, R. (2021). A framework to manage smart educational certificates and thwart forgery on a permissioned blockchain. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.01.740

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Emn178. (2017, December 18). *js-sha256*. Git Hub. https://github.com/emn178/js-sha256

expressjs. (2010, November 16). *Express*. Git Hub. https://github.com/expressjs

Grolleau, G., Lakhal, T., & Mzoughi, N. (2008). An Introduction to the Economics of Fake Degrees. *Journal of Economic Issues*, *42*(3), 673–693. https://doi.org/10.1080/00213624.2008.11507173

Haddouti, S. el, & Ech-Cherif El Kettani, M. D. (2019). Analysis of identity management systems using blockchain technology. *Proceedings - 2019 International Conference on Advanced Communication Technologies and Networking, CommNet 2019*. https://doi.org/10.1109/COMMNET.2019.8742375

Heredia, A., Barros, M.-J., & Barros-Gavilanes, G. (2022). *Decentralizing Certificates Issuance Through Blockchain*. 1–6. https://doi.org/10.1109/icecet52533.2021.9698558

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH 1. In *Design Science in IS Research MIS Quarterly* (Vol. 28, Issue 1).

Huynh, T. T., Tru Huynh, T., Pham, D. K., & Khoa Ngo, A. (2018). Issuing and Verifying Digital Certificates with Blockchain. *2018 International Conference on Advanced Technologies for Communications (ATC)*, 332–336. https://doi.org/10.1109/ATC.2018.8587428

Hyperledger Foundation. (2022). *Hyperledger Fabric*. https://www.hyperledger.org/use/fabric

jQuery. (2006, January 14). *jQuery*. https://github.com/jquery/jquery

Kim, C. (2020). *Ethereum 2.0: How it works and why it matters*.

Marella, V., & Vijayan, A. (2020). Document Verification using Blockchain for Trusted CV Information. *AMCIS 2020 Proceedings*. https://aisel.aisnet.org/amcis2020/adv_info_systems_research/adv_info_systems_research/12

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

MetaMask. (2019, May 21). *Metamask-extension*. https://github.com/MetaMask/metamask-extension

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org

Nguyen, B. M., Dao, T. C., & Do, B. L. (2020). Towards a blockchain-based certificate authentication system in Vietnam. *PeerJ Computer Science*, *2020*(3). https://doi.org/10.7717/PEERJ-CS.266

Nodejs. (2009, May 27). *Node*. Git Hub. https://github.com/nodejs/node

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business and Information Systems Engineering*, *59*(3), 183–187. https://doi.org/10.1007/S12599-017-0467-3/TABLES/1

Pfefferling, A., & Kehling, P. (2021). *Design disclosure for Blockchain-based Application used in public education certificates with electronic hashes*. *004*, 034 – 041. https://doi.org/10.48446/opus-13094

Reddy, T. R., Reddy, P. V. G. D., Srinivas, R., Raghavendran, Ch. v., Lalitha, R. V. S., & Annapurna, B. (2021). Proposing a reliable method of securing and verifying the credentials of graduates through blockchain. *EURASIP Journal on Information Security*, *2021*(1), 7. https://doi.org/10.1186/s13635-021-00122-5

Serranito, D., Vasconcelos, A., Guerreiro, S., & Correia, M. (2020). Blockchain Ecosystem for Verifiable Qualifications. *2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2020*, 192–199. https://doi.org/10.1109/BRAINS49436.2020.9223305

SheetJS. (2014, May 22). *SheetJS*. https://github.com/SheetJS/sheetjs

Solat, S., Calvez, P., & Naït-Abdesselam, F. (2021). Permissioned vs. Permissionless Blockchain: How and Why There Is Only One Right Choice. *Journal of Software*, 95–106. https://doi.org/10.17706/jsw.16.3.95-106

Sun, H., Wang, X., & Wang, X. (2018). Application of blockchain technology in online education. *International Journal of Emerging Technologies in Learning*, *13*(10), 252–259. https://doi.org/10.3991/ijet.v13i10.9455

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475–491. https://doi.org/10.1016/J.FUTURE.2019.12.019

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt