UNIVERSITY OF THESSALY

Diploma Thesis

Academic Certificates Delivery Application through Blockchain

Author:
Konstantina Tsakiri

Supervisors:
Dimitrios Katsaros
Athanasios Korakis

A thesis submitted in fulfillment of the requirements for the bachelor degree of Computer and Communication Engineer

in the

Department of Electrical & Computer Engineering

July 2018

“*Φτᾶσε ὅπου δὲ μπορεῖς !*”

Νίκος Καζαντζάκης

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Περίληψη

Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Διπλωματική Διατριβή

Εφαρμογή Παράδοσης Ακαδημαϊκών Πιστοποιητικών μέσω της τεχνολογίας Blockchain

Κωνσταντίνα Τσακίρη

Η Τεχνολογία Blockchain είναι ένας εξελισσόμενος τομέας, ο οποίος αναπτύχθηκε γρήγορα τα τελευταία χρόνια με αφορμή την έλευση των κρυπτονομισμάτων. Η “καρδιά” αυτής της τεχνολογίας, η οποία ήρθε στο φως με την εμφάνιση του πιο γνωστού έως τώρα κρυπτονομίσματος, του Bitcoin, έχει ήδη εφαρμοστεί σε πολλά, καθώς και διαφορετικά, πεδία και προβλέπεται να επεκταθεί ολοένα και περισσότερο. Το Bitcoin ήταν μόνο η αρχή κι ενδεχομένως ένα έναυσμα για να γίνει περαιτέρω έρευνα στην τεχνολογία πίσω από αυτό, την τεχνολογία Blockchain. Η παρούσα διπλωματική διατριβή, αρχικά εισάγει μία σύντομη βιβλιογραφική ανασκόπηση του Blockchain, παρουσιάζει μερικές σημαντικές εφαρμογές, κυρίως συναφείς με τον τομέα της εκπαίδευσης και τέλος, επικεντρώνεται στην παρουσίαση της εφαρμογής μας, η οποία εκδίδει Ακαδημαϊκά Πιστοποιητικά μέσω της προηγμένης τεχνολογίας Blockchain.

UNIVERSITY OF THESSALY

Abstract

Department of Electrical & Computer Engineering

Diploma Thesis

Academic Certificates Delivery Application through Blockchain

Konstantina Tsakiri

Blockchain Technology is an evolving field that developed rapidly over the last years, driven by the emergence of cryptocurrencies. The core technology, which underpins the most famous cryptocurrency, bitcoin, has already been applied in many areas and is foreseen increasingly expansion. Bitcoin was just the beginning and possibly a trigger for research into the technology behind it, Blockchain technology. This diploma thesis, initially introduces an overview of blockchain, presents some fruitful applications, mainly for education and focuses on our application, which issues and delivers Academic Certificates through Blockchain.

Acknowledgements

First and foremost I would like to thank my supervisors, Assistant Professor Dimitrios Katsaros, who gave me the opportunity to deal with a state-of-the-art topic and for all his help and Assistant Professor Athanasios Korakis as my second supervisor.

Off course, I am more than grateful to my mother *Kassiani* for all her support and to my brother *Ioannis* who is always there for me and has an answer for all my inquiries.

Finally, I want to thank all those who were close to me with their unselfish love throughout this long journey.

Dedicated to my father, *Dimitris*.

Contents

List of Figures

List of Abbreviations

CV	Curriculum Vitae
CSV	Comma-separated Values
FOSS	Free and Open-Source Software
GDPR	General Data Protection Regulation
IoT	Internet of Things
JSON	Javascript Object Notation
MIT	Massachusetts Institute of Technology
PDF	Portable Document Format
PoW	Proof-of-Work
P2P	Peer-to-peer
PoS	Proof-of-Stake
RPC	Remote Procedure Call
SHA	Secure Hash Algorithm
UCL	University College London

Glossary of terms

Bitcoin:
The name of a decentralized digital currency created by unknown Satoshi Nakamoto

Bitcoin address:
A bitcoin address is an identifier of 26-35 alphanumeric characters starting with number “1” that represents a possible destination for a bitcoin transaction

Bitcoind:
Bitcoind is a program that implements the Bitcoin protocol RPC use

Block:
A grouping transactions, marked with a timestamp and a fingerprint of the previous block. The block header is hashed to find a proof-of-work, thereby validating the transaction. Valid blocks are added to the main blockchain by network consensus

Blockchain:
A list of validated blocks

Cryptography:
Cryptography is the practice and study of techniques for secure communication in the presence of third parties.

Docker:
Docker is a tool designed to create, deploy, and run applications by using containers

Docker container:
Docker container is used to run Bitcoin in regtest mode

Double-spending:
Spendind the same amount of bitcoin more than once

Hash:
A digital fingerprint of some binary input

Merkle tree:
Merkle tree is a binary tree containing cryptographic hashes used for efficiently summarizing and verifying the integrity of large sets of data

Metadata:
Metadata is data that provides information about other data. It may include elements such as title, abstract, author, and keywords.

Miner:
A network node that finds valid proof-of-work for new blocks, by repeated hashing

Nonce:
In cryptography, nonce in a bitcoin block is a 4-byte field that can be used just once. It is issued in an authentication protocol

Open standard:
An open standard is a standard that is publicly available and has various rights to use associated with it

Private key:

A private key is used to generate a signature for each blockchain transaction a user sends out

Public key:
Public key is an address in a transaction

Proof-of-work:
A piece of data that requires significant computation to find

Reward:
An amount included in each new block as a reward by the network to the mine who found the PoW solution

SHA-256:
SHA-256 is a hash algorithm which produces a 256-bit number

Smart contracts:
Smart contracts are contracts with the terms of the agreement between two parties being written into lines of code

Tamper-proof:
The meaning of the word tamper-proof is “impossible to change”

Transactions:
Transactions are data structures that encode the transfer of value between participants in the bitcoin system

Chapter 1

Introduction

In this introduction chapter we approach the main topic of this thesis, that is the Blockchain Technology and the way in which it can be utilized by building an application for academic certificates delivery. First, we will discuss the current situation, and subsequently, we will refer to the possible development in less common fields so far that could affect institutions, as Universities, to be more transparent, inclusive and accountable. Finally, we will state our contribution in order to give a solution and different approach for the issuance of academic certificates.

Figure 1.1: Block chain

1.1 Current Situation

Throughout the first half of the 21st century, humanity has been overwhelmed by technological revolutions that has already a major impact and will change furthermore our life from the way we transact money, vote or even prove who we are. Nowadays, there is a lot of hype around Blockchain technology which is exploding by virtue of Bitcoin and is fundamentally changing in general the business landscape [1]. Especially, someone could conceptualize the use of Blockchain to Bitcoin, if he compares corresponding to what the Internet is for the email. Many of what are being done and are heard today around Blockchain reminds what happened with the Internet in the 1990s and thus is considered that this technology is the most significant invention since the advent of Internet and electricity itself [2].

Blockchain may be defined as an electronic system, where a variety of applications could be built. Actually, the decentralized mechanism allowed by blockchain is applicable in a number of domains to monitor all online transactions - such as contracts, tasks, payments - that have become ubiquitous in everyday life.

Although, in any kind of transaction, a third trusted entity is required, it can be replaced by a properly designed Blockchain application. As Iansiti and Lakhani explain in the Harvard Business Review [3], the need for intermediaries, including institutions, lawyers, bankers, would be obsolete and everyone could trade efficiently with security, avoiding the possibility of fraud. By enabling the storage of the records in a distributed ledger, blockchain is driving a fundamental shift from the Internet of information, where everyone can look around, exchange and communicate information to the Internet of value, where everyone can contribute to something important.

Although, the first blockchain was conceptualized ten (10) years ago and was implemented in 2009, the invention of the bitcoin design is causing increasingly the inspiration for more applications from various communities. Nowadays, there is a growing interest about the "buzzword" blockchain because it was soon realized that the potential of this distributed architecture could go far beyond the use of virtual money [4]. To date, there are blockchain-based applications for online voting, health issues, smart contracts, and proof of ownership. For instance, many projects are working in order to provide personal digital identities [5], even though few of the existing applications are correlated to the Universities.

Blockchain technology accelerates decentralized identity models by providing a web of trust as people, organizations and connected devices establish and share their own identity created by them and verified by relationships, which solves digital identity management. Aside from identities, everyone could also prove additional information for himself, such as credentials or anything of value. As education becomes more decentralized and equaled for all, researchers and institutions should consider how the blockchain technology could be integrated to maintain reputation, proof of knowledge and trust in certification.

This diploma thesis aims to overview that aforementioned technology and to propose our application in order to examine how the Universities and the related institutions should approach and be consistent with this latest and advanced technology. Also, through this thesis is provided a solution with which is enabled an efficient and reliable way to verify academic certificates.

1.2 Thesis contribution

This thesis presents the implementation of an application, which issues and verifies academic certificates. This application will enable students to receive every document related to student affairs, such as diploma certificates, certificates of study, transcripts which until now is provided and is issued by the Secretariat of each Department in the University, without having to go to the issuing authority, therefore without the need of an intermediary. In particular, these records could be transmitted directly to the student or to an alumni and they would own and share their official records in a manner that is initially trustworthy, safe, and tamper-proof.

However, blockchain adoption and use in the context of Universities does not convey the abolition of the Universities' Administrative Offices because their existence is essential for the proper operation. The target of our application is not one-sided, basically is to benefit every student with verifying immediately every certificate they need and then, to minimize and improve the functions, which are in charged the Secretariat. For instance, they have to maintain extensive databases

that most of them are paper-based, so the importance to be digitized is imperative rather than to be stored in immutable and distributed ledgers [6]. Not only may interest Universities, but also every institution imparting certificate courses, employers and professional certification bodies. For instance, companies could have a benefit from our application because through a "digital diploma" they would verify immediately the accuracy of the qualifications of the nominee employee without having to contact with each University.

Certificates play an important role in education and companies, where individual learning records become essential for people's professional careers. In our case, the accomplishment of the application uses the Bitcoin blockchain over Blockcerts for issuing and verifying in trustless way blockchain-based official records [7]. The certificate data would be added to the blockchain by the awarding institution in which the student can access, share with employers or link from an online resume.

The contribution of thesis not only provides a better solution for the delivery of academic certificates, but it is also a step closer to a way, which would be very possible figuratived in the future.

1.3 Thesis contribution

This diploma thesis is organized as follows:

Chapter 1 presents an introduction about the era of Blockchain technology and its extensions which could be applied in many areas and especially in the higher education that is the purpose of our contribution.

Chapter 2 provides a review of the Blockchain through the theoretical background and the related work that has already been accomplished in the same field.

Chapter 3 deals with the implementation and the technologies, which are used for this.

Chapter 4 summarizes the benefits of this app and suggest further research in order to provide an complete solution that could be utilized from the interested parties, especially Universities in Greece.

Chapter 2

Literature review

This chapter outlines an overview of Blockchain technology and presents the prior related attempts.

2.1 Blockchain Technology Overview

Historically, when it comes to transacting money or anything of value, people have relied on intermediaries like banks and governments to ensure trust and certainty. The first banks held notes or books with the clients' transactions and this basic system was based on trust and the solvency of it. The need for middlemen is especially acute when making a digital transaction because digital assets like money, stocks and intellectual property are essential files, they are incredibly easy to reproduce. This has created the double-spending problem, which is the act of spending the same unit of value more than once and has prevented the peer-to-peer transfer of digital assets.

In October 2008, Satoshi Nakamoto, which is a pseudonym for the author, whose identity is currently unknown, published a white paper with the title: "Bitcoin: A Peer-to-Peer Electronic Cash System" . The paper described a new method for creating a fully distributed digital currency system by cryptographically chaining blocks of data together and, in particular, they proposed a solution to the double-spending problem using public-key cryptography in a peer-to-peer network, whereby each user is assigned a private key and a public key is shared with all other users [1], [8]. This technique was originally described in 1991 by a group of researchers and it was originally intended to timestamp digital documents so it not possibly to tamper with them almost like a notary [9]. However, it was mostly unused until the adoption of it by Satoshi Nakamoto to create something innovative that provides a method for abstracting value, assigning ownership, and providing a means for transacting [10].

Figure 2.1: Blockchain Technology

According to the description of Blockchain that was given from the bitcoin wiki [11], it is defined as a persistent, tamper resistant, secure database that are composed from blocks, which are linked and secured due to cryptography and its distributed character.

More specifically, the structure of a block, as it is obvious in the Figure 2.2, contains a block header and a list of transactions associated with the respective block. Firstly, the block header has a hash which has analogous function with a fingerprint because it is unique, and is calculated when a block is created. The hashes are also important at detecting changes to a block, by checking if its fingerprint has changed. At the inner of a block header there are the main components that are used in the mining process, as seen in the Figure 2.3 below:

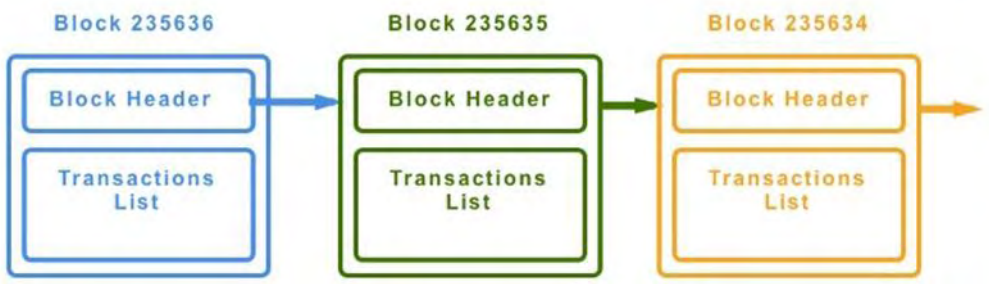


Figure 2.2: Block's Components

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the Merkle-Tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The Proof-of-Work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

Figure 2.3: Structure of block header

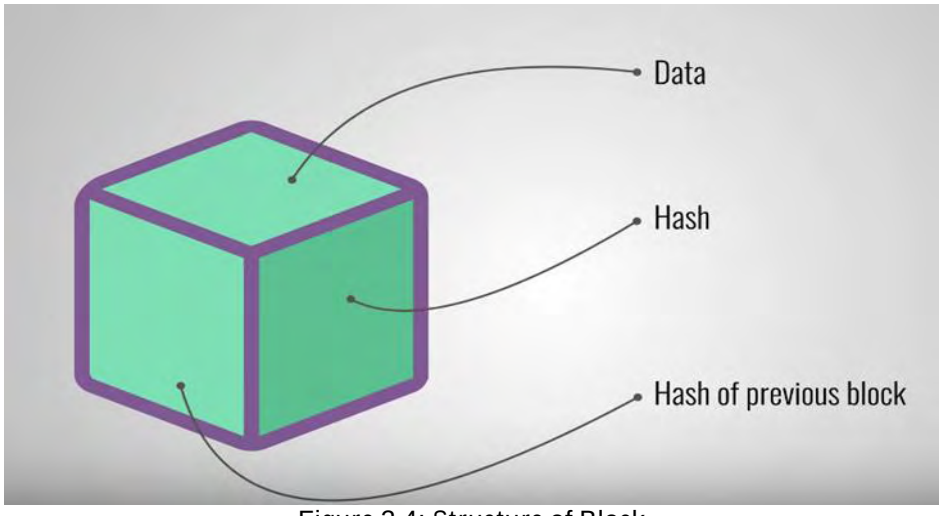


Figure 2.4: Structure of Block

The hash of the previous block defines that a block has only one parent block except from the first block of a blockchain that is called genesis block or block 0 and it has no parent block as there is no prior hash [13]. If one block of the chain is tampered with, its hash should change as well and respectively all following blocks will become invalid because they do not store anymore a valid hash of the previous block. So, the utilization of hashes is not sufficient to prevent tampering and the design of blockchain has "proof-of-work" to mitigate this problem.

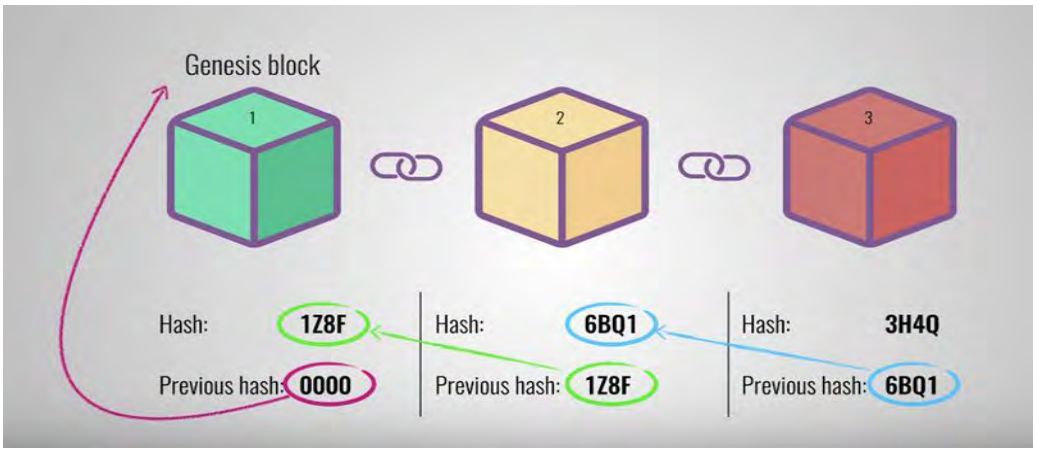


Figure 2.5: Chain of Blocks

Proof-of-Work is a mechanism that slows down the creation of new blocks. In the case of Bitcoin, it lasts about ten (10) minutes to calculate the required PoW and add a new block to the chain. So, the security of a Bitcoin blockchain is based on its creative use of hashing and the PoW mechanism. Additionally, blockchains secure themselves by being distributed and instead of using a central entity to manage the chain, blockchain uses a P2P network where everyone is allowed to join and when he joins it, he gets the full copy of the network. The node can use this copy for the verification that everything is in order.

Subsequently, when someone creates a new block this one is send to every node on the network and then each of them verifies the block to make sure that it has not been tampered with. If everything checks out, each node adds this block to their own blockchain. As a result, all the nodes in this network create consensus because they agree about what blocks are valid and what they are not. Moreover, to accomplish tamper with a blockchain, you will need to tamper with all blocks on the chain, redo the proof-of-work for each block and take control of more than 50% of the P2P network and finally your tampered block will be accepted by everyone else.

Furthermore, the idea of PoW was first introduced in 1993 to combat spam emails and was formally called with this name from 1997 [14]. The way that works is by having all nodes solve a cryptographic "puzzle". This puzzle is solved by miners and the first one to find the solution gets the miner reward. According to Digiconomist [15], Bitcoin miners uses enormous amount of electricity, enough to power entire countries and if "Bitcoin" was a country, it would rank as shown in the Figure 2.6 below. PoW gives more rewards to people with bigger computational power and better equipment and due to the higher your hash rate is, the higher the chance that you will get to create the next block and receive the mining reward. To increase these chances, miners have come together in what is called "mining pools", where they combine their hashing power and distribute the reward evenly across everyone in the pool.

To sum it up, PoW is causing miners to consume amounts of energy and with the use of mining pools the blockchain become more centralized as opposed to decentralized. There are also other consensus algorithms that could be more

effective that PoW, for instance Proof-of-Stake.

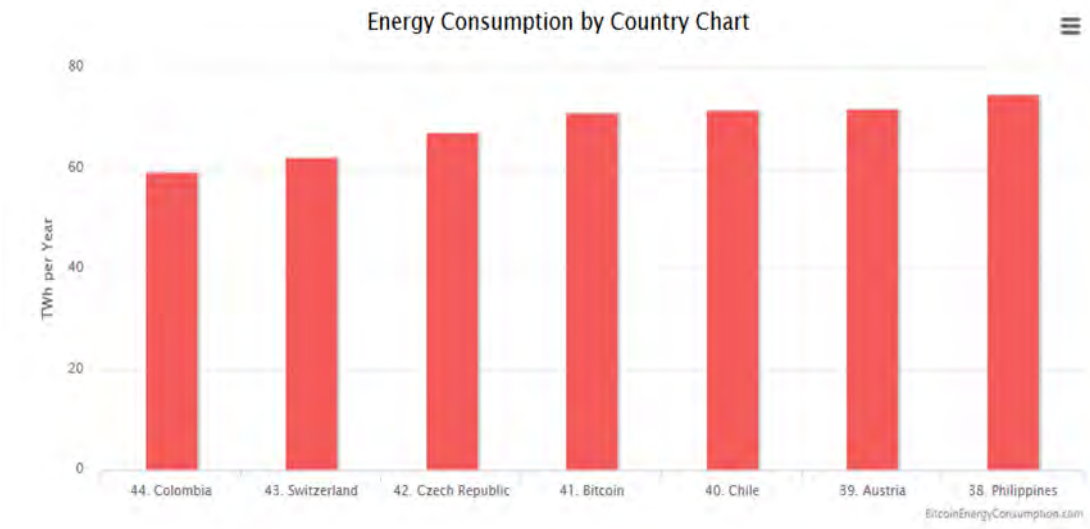


Figure 2.6: Energy Consumption of Bitcoin

The blockchain technology is constantly evolving and until now there are three (3) generations of blockchains [8]:

1. Blockchain 1.0 for digital currency
2. Blockchain 2.0 for digital finance
3. Blockchain 3.0 for digital society

In detail, Blockchain 1.0 started with the birth of Bitcoin in 2008 and has already an economic impact, in contrast with Blockhain 2.0 and Blockchain 3.0 that count less than three (3) years.

Figure 2.7: Globally Interest over Last year

According to Google trends, we can observe in the Figure 2.7 the hype around blockchain over the last year, which is peaked in the last week of 2017. Even more remarkable, is to see how many people have searched about Blockchain since the advent of Bitcoin. As is shown in Figure 2.8 below, there is non-existent interest before 2013 and from then is observed exponential activity.

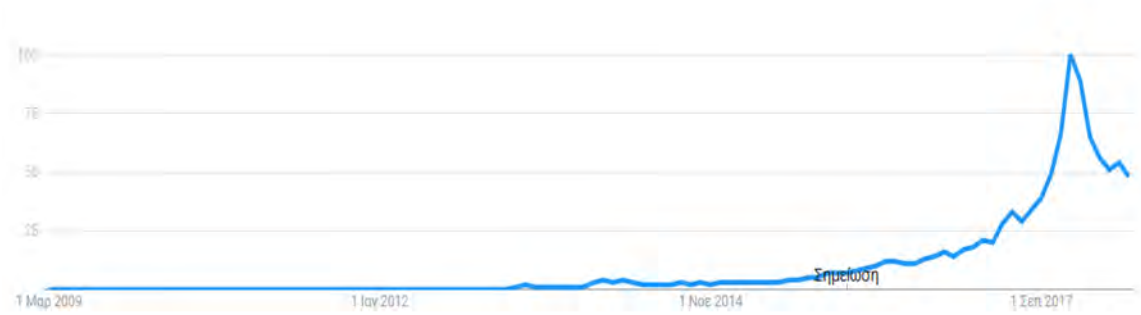


Figure 2.8: Interest over time

From the Figures 2.7, 2.8, it is verified that this disruptive technology deserves our attention and will penetrate into society with increasing progress and as well could be soon completely instituted.

2.2 Related work

As discussed in section 1.1 blockchain has applications that go beyond obvious things like digital currencies and transfers of money. We are walking into the Blockchain 3.0 generation which means that the digital society is searching for applications in new areas, such as smart cities, IoT, education, government, health, science and art.

Figure 2.9: Related work

The above Figure 2.9 points out the places around the world, where are working on corresponding projects with this thesis. Initially, it is essential to refer how the Blockcerts has been created since we rely on it. In 2015, Phillipp Schmidt, the director of learning innovation at the MIT Media Lab had begun issuing non-academic digital certificates on a small scale and a bit later, throughout 2016 with the contribution of Learning Machine, an education technology company and the team of MIT Media Lab is developed an open-source toolkit called Blockcerts [16], [17]. Officially, MIT has begun issuing digital diplomas that are registered on the Bitcoin blockchain in order to be shared verified by every peer.

Another remarkable case is the University of Nicosia in Cyprus that is, in general, a pioneer in blockchain technology and the first higher education institution to issue academic certificates into Bitcoin's blockchain from 2014. Until last year, the graduates get not only a physical diploma but also, from the Spring of 2017, receive a copy of their diploma in a PDF format, which has special metadata that anchors that certificate into the blockchain using a fingerprint of the PDF [18]. In this way, a diploma is validated that was indeed published by the University of Nicosia and timestamped by Bitcoin's blockchain. Moreover, University of Nicosia stands out as well is the 1st University globally that offers a degree in Digital Currency and accepts Bitcoin as a form of tuition fee payment.

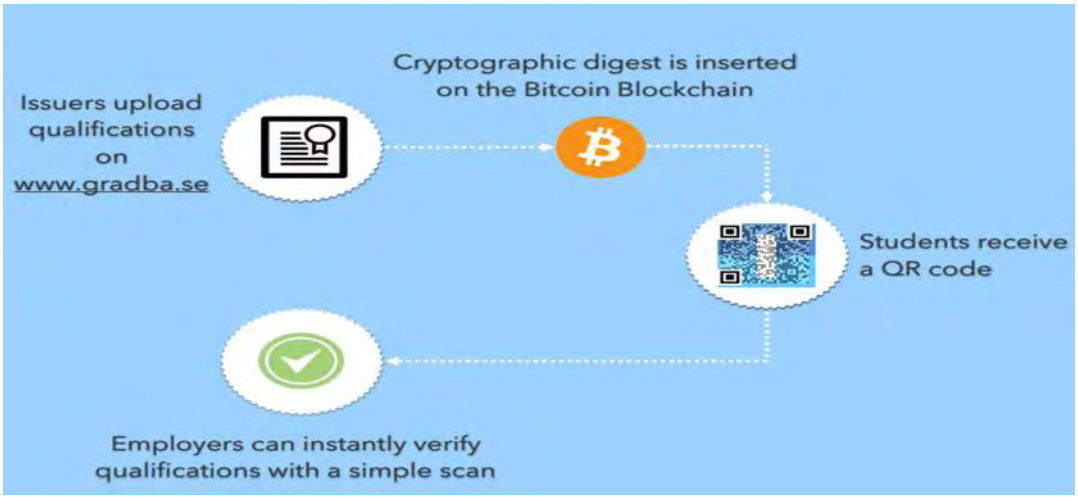


Figure 2.10: How Gradbase works

As a survey by CareerBuilder in the United Kingdom has shown [19], has been revealed that 56% of hiring managers have found that job nominees lying for their skills on their resumes and is expected that is time consuming for the employers to check everyone's CV. Based on this, Gradbase has the target to tackle CV fraud with the Bitcoin Blockchain and guarantees that anybody, anywhere can instantly verify the true qualifications [20]. In the Figure 2.10 is shown the way that Gradbase works. What is more, Gradbase collaborates with UCL Centre for Blockchain Technologies in order to prove that every MSc graduate in Financial Risk Management has an authentic degree.

The most recently and relevant attempt is implemented in a pilot way by the government of Malta for putting academic certificates on a Blockchain working with Learning Machine Technologies, such as the MIT Media Lab, and utilizing over the open standard of Blockcerts. The choice of this small country could not be considered accidental as Malta is located in a nodal place and is among the countries with the most refugees per capita. Historically, this refugee population is the most highly educated and they can not document their achievements, so it could be described as human tragedy. As a result, this program emphasizes on refugees in order to prove their educational knowledge and help them to find a relevant job activity [21]. Finally, we were inspired by this use case and absolutely, could be an example in order to adopt similar programs.

Chapter 3

Implementation

This chapter explains the procedure that have been implemented in order to build our application through Blockcerts and achieve our goal that issues and verifies academic certificates due to Blockchain technology.

3.1 Design Overview

Blockcerts is published under the MIT FOSS License [22], so it means that is free and available for everyone to use it as a first step to build his own app for issuing, displaying and verifying digital official records. In our case, due to Blockcerts and its open-sourced libraries and tools, the academic certificates can be registered on the Blockchain, being cryptographically signed, tamper-proof and shareable providing and facilitating individuals to directly own their digital records they need without a third entity.

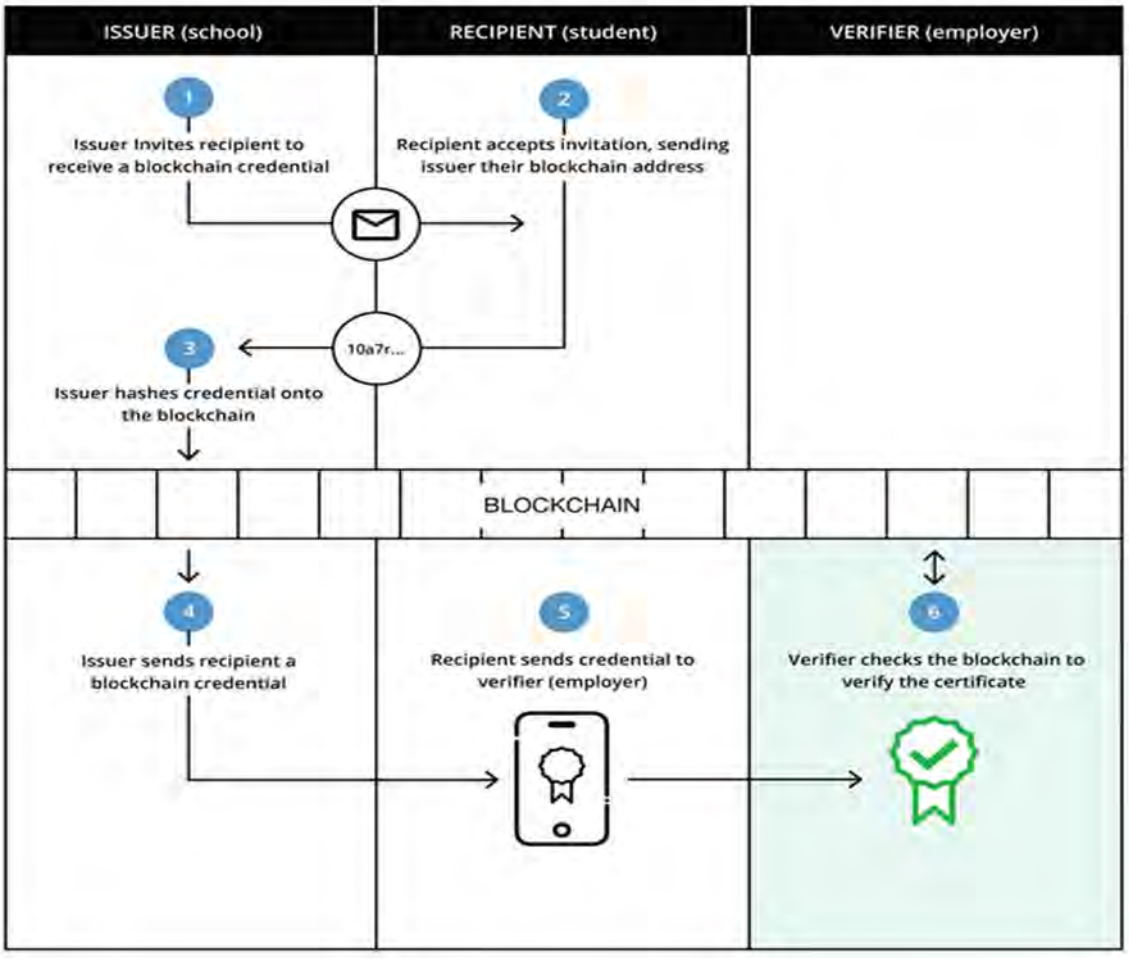


Figure 3.1: Design of Application

One important specification is the need of a recipient-centric ecosystem as we can see in the Figure 3.1 and we are based on it for our implementation.

According with the design of our solution, there are three (3) participants: the issuer that is the Secretariat for our case, the recipient who can be every student of the Department and the verifier, who could be a willing employer. In general, the required steps to follow are five (5):

1. Issuer invites recipient to receive a blockchain credential
2. Recipient accepts invitation by sending to the issuer his blockchain address
3. Issuer hashes the credential onto the blockchain
4. Issuer sends to the recipient the blockchain credential
5. Recipients owns the credential and he can share it with the verifier who can confirm the certificate by checking the blockchain

The design is consisted mainly of two components, the issuing and the verifying part. In detail, the issuer in order to issue, for instance a diploma certificate, on the blockchain has to do the following:

- Creation of a JSON file, which includes the standard description of an University diploma such as the name of the University, the name of the graduate and the degree of diploma
- Calculation of the hash with SHA-256 algorithm of the JSON file created above to ensure that it would not be tampered with [22]
- Issue a blockchain transaction from the issuer's blockchain address to the graduate's

After those steps, the blockchain transaction is completed with a valid hash. Secondly, the verifying component is essential when a verifier - very possible an employer- have to make sure that the employee nominee has the qualifications listed on his resume, in particular that really owns the diploma for the specific University which is mentioned.

The recipient shares with the verifier the JSON file, a file whose content is notarized and "sealed", containing the data regarding the certificate itself and the blockchain address of the transaction. With these elements, the verifier could get that valid hash of the transaction, calculate the hash of the JSON file and in this manner, verify that this digital record which is indicated in the resume is the same with the diploma certificate that is issued from the University.

Practically, except for the JSON file, we need to provide Recipients Roster, a roster.csv file, that includes the fields with the name of a graduate, identity, public key and it is a primary step for the creation of a certificate, as seen in the Figure 3.2 below. Also, we see a third necessary component in order to create the unsigned certificates, cert-tools.

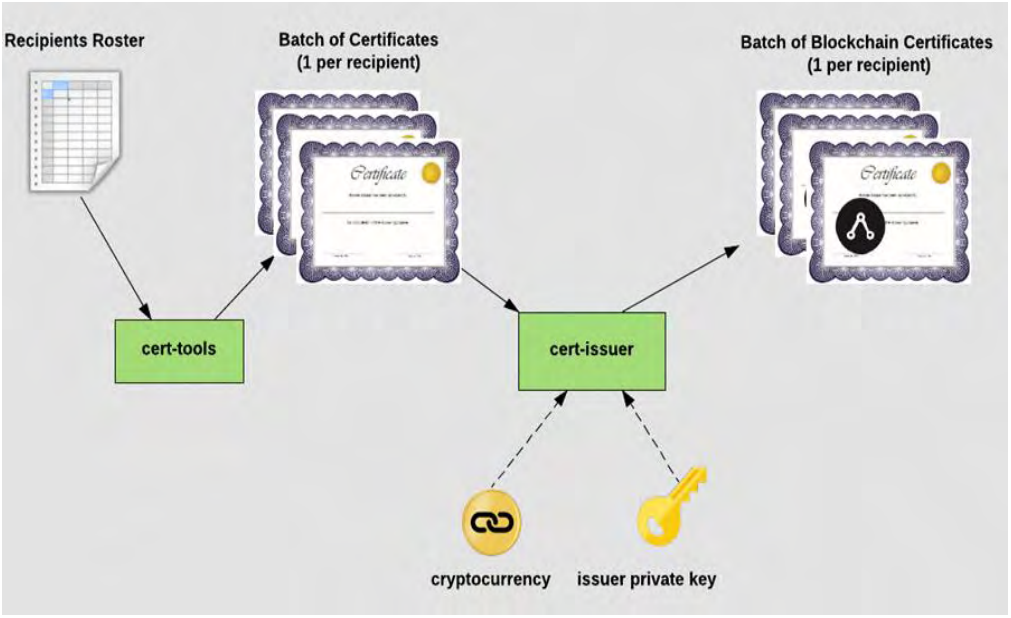


Figure 3.2: Design Components

3.2 Development

In this subsection it is described the repositories that are composed for the development of the application on Ubuntu Linux testing environment.

A. Cert-tools: Creation of "unsigned_certificates"

Firstly, the building of the application requires the installation of virtualen that is a tool to create isolated Python environment. Cert-tools from the above Figure 3.2 is necessary because it contains two scripts for designing the template of a certificate and the instantiating of a certificate batch.

These scripts are:

- create_certificate_template.py
- instantiate_certificate_batch.py

1. Activate python environment:

   - *source ./venv/bin/activate*

2. Creation of the file "template" that will be in the folder certificate_templates with running the command:

   - *create-certificate-template –c givenname.ini*

   The name of JSON file that is created it depends in the name we give at the field "template_file_name" of the file "givenname.ini"

With the script for the instantiation, a certificate per recipient is generated based on the values in the csv file.

B. Cert-issuer: Digital signature of certificates

Cert-issuer part issues blockchain certificates by creating a transaction from the issuing institution to the recipient on the Bitcoin blockchain that includes the hash of the certificate itself. Starting using Docker container in Ubuntu, which configures the development environment with a test blockchain.

1. Initially, we want to get the Docker image so, we build a docker container from the directory with the folder cert-issuer with the command:

   - *docker build –t bc/cert-issuer:1.0 .*

2. Also, we can create a snapshot of our docker container, finding the "container_id" of the process with the below commands:

   - *docker ps –l*
   - *docker commit <container for your bc/cert-issuer> my_cert_issuer*

3. Subsequently, we run the bitcoin server:

   - *docker run -it bc/cert-issuer:1.0 bash*

4. After we ensure that the docker image is running and bitcoind process is started, the following step is to create an issuing address in an experimenting way:

   - *issuer= `bitcoin-cli getnewaddress`*
   - *sed –i.bak "s/<issuing-address>/$issuer/g" /etc/cert-issuer/conf.ini*
   - *bitcoin-cli dumpprivkey $issuer > /etc/cert-issuer/pk_issuer.txt*

   The *dumpprivkey* command extracts the private key that was generate by the *getnewaddress* command. In this way, it is possible for bitcoind to know the private key from the public key.

5. We copy the ".json" files from the folder "unsigned_certificates". This have to be done from a new terminal, where we will activate again python environment as we do in the A.1 step and we will find out the container id as the B.2 step:

   - *docker cp ./cert-tools/certificate-data/unsigned_certificates givenname.json container_id:/etc/cert-issuer/data/unsigned_certificates*

6. After issuing certificates, we need enough BTC in our issuing address and we will use bitcoind in regtest mode, a test issuing mode, in order to print fake money, especially 50 BTC:

   - *bitcoin-cli generate 101*
   - *bitcoin-cli getbalance*
   - *bitcoin-cli sendtoaddress $issuer 5*

7. Now, we can issue the certificate on the blockchain running:

- *cert-issuer –c /etc/cert-issuer/conf.ini*

8. The Blockchain certificate is located in /etc/cert-issuer/data/blockchain_certificates. By copying this to our local machine, we add it to cert-viewer's "cert-data" folder to see the certificate:

   - *docker cp container_id:/etc/cert-issuer/data/blockchain_certificates .*

C. Cert-viewer

After the certificate is issued, cert-viewer is used to display and verify it. Through this repository, we can request certificates and generate a new Bitcoin identity. We run the below commands in order to view the certificate:

- *Python run.py –c conf_local.ini*
- *http://localhost:5000*

3.3 Example of Academic Certificate

In this subsection we deliver an academic certificate through Blockchain, following the aforementioned implementation. Especially, this use case is about the certification of graduation from the Department Electrical and Computer Engineering, University of Thessaly and its creation is mainly based on the JSON file. The Figure 3.4 indicates the format of the file that defines the display of diploma certificate.

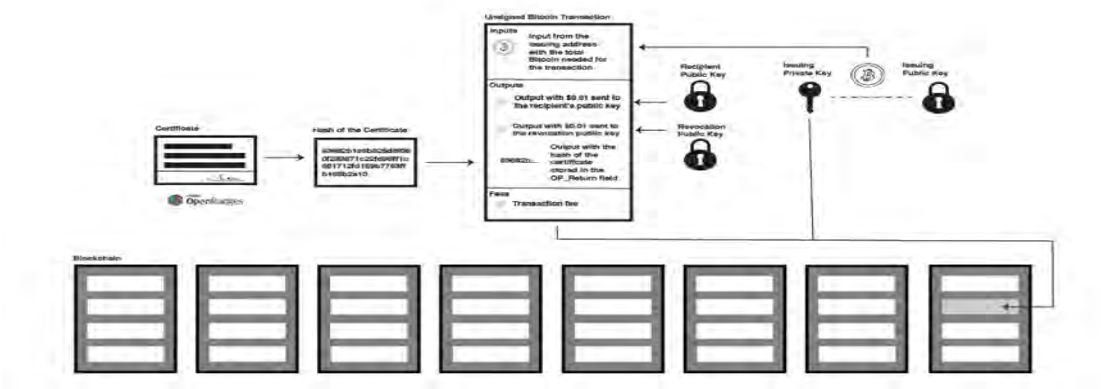
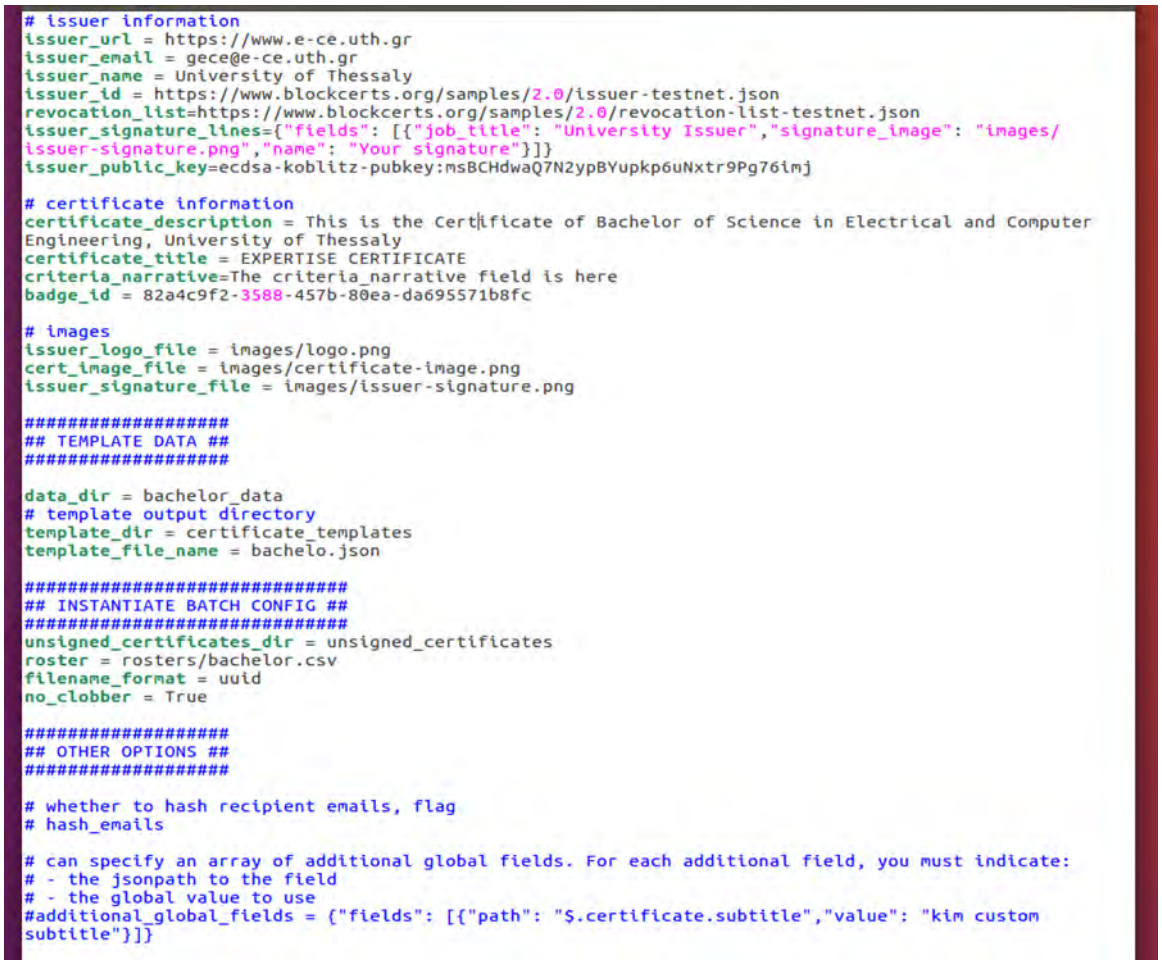


Figure 3.3 Design of blochain-based certificates



```
# issuer information
issuer_url = https://www.e-ce.uth.gr
issuer_email = gece@e-ce.uth.gr
issuer_name = University of Thessaly
issuer_id = https://www.blockcerts.org/samples/2.0/issuer-testnet.json
revocation_list=https://www.blockcerts.org/samples/2.0/revocation-list-testnet.json
issuer_signature_lines={"fields": [{"job_title": "University Issuer","signature_image": "images/
issuer-signature.png","name": "Your signature"}]}
issuer_public_key=ecdsa-koblitz-pubkey:msBCHdwaQ7N2ypBYupkp6uNxtr9Pg76imj

# certificate information
certificate_description = This is the Certificate of Bachelor of Science in Electrical and Computer
Engineering, University of Thessaly
certificate_title = EXPERTISE CERTIFICATE
criteria_narrative=The criteria_narrative field is here
badge_id = 82a4c9f2-3588-457b-80ea-da695571b8fc

# images
issuer_logo_file = images/logo.png
cert_image_file = images/certificate-image.png
issuer_signature_file = images/issuer-signature.png

####################
## TEMPLATE DATA ##
####################

data_dir = bachelor_data
# template output directory
template_dir = certificate_templates
template_file_name = bachelo.json

##############################
## INSTANTIATE BATCH CONFIG ##
##############################
unsigned_certificates_dir = unsigned_certificates
roster = rosters/bachelor.csv
filename_format = uuid
no_clobber = True

####################
## OTHER OPTIONS ##
####################

# whether to hash recipient emails, flag
# hash_emails

# can specify an array of additional global fields. For each additional field, you must indicate:
# - the jsonpath to the field
# - the global value to use
#additional_global_fields = {"fields": [{"path": "$.certificate.subtitle","value": "kim custom
subtitle"}]}
```

Figure 3.4: Format of file

According to the Figures 3.3, 3.4 and through the JSON file, is created the hash of the certificate and the certificate is issued onto the Bitcoin blockchain. Due to cert-issuer tool, we are allowed to experiment with test mode through configuration option. The final certificate will be ready, if you browse on: http://localhost:5000 and it would be as to the Figure 3.5.

Figure 3.5: Academic Certificate through Blockchain

As we can see in the Figure 3.5 that shows a screenshot of the final step of application, there is a button “Verify certificate”. The verification is the last step of the process, as is shown in the Figure 3.6 below.

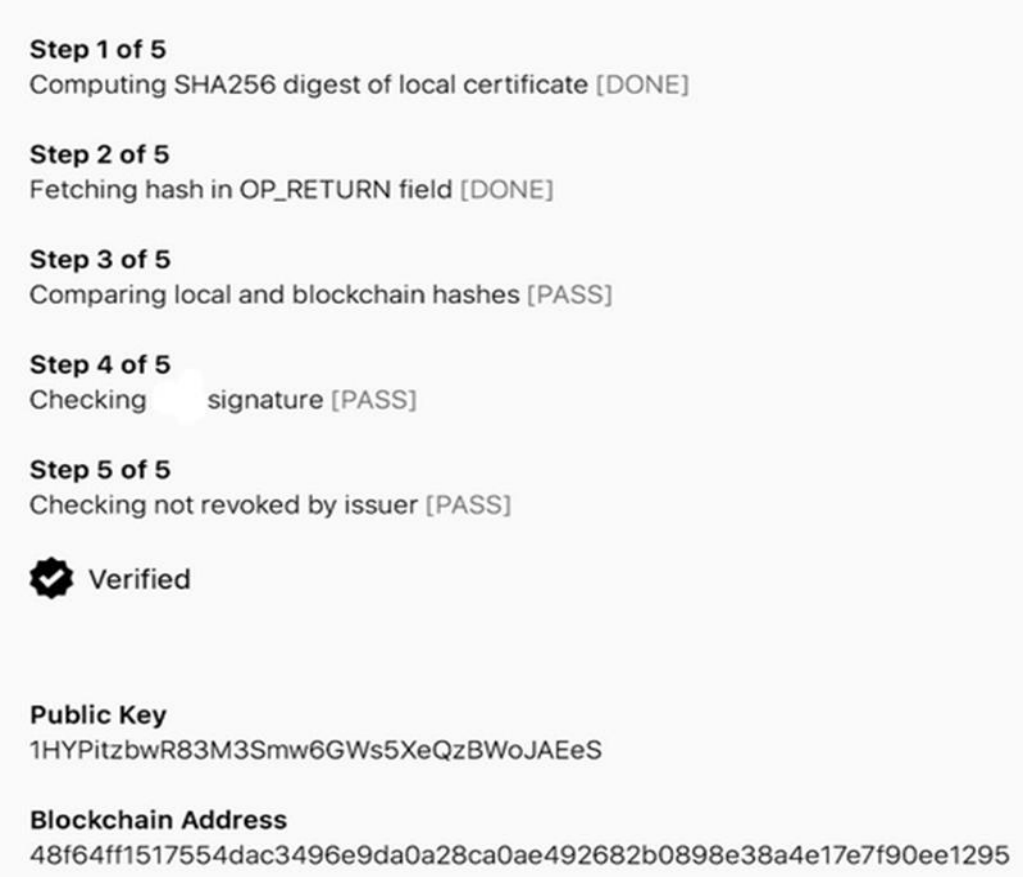


Figure 3.6: Verification of certificate

This certificate would actually be signed by the issuing institution, University of Thessaly, with their public key that encrypts the hash of the certificate.

Examining the case if someone wants to counterfeit a corresponding diploma, he would make a same in appearance but it could easily identified as a fake because the public key will not recognized as the official one. The part of identification is not something new, it is mathematically possible to determine whether an issuer's legitimate or not.

A reasonable question about this diploma, or about every certificate that may be issued with this application, is if the certificate can be revoked. The answer is affirmative whereas it can be programmed to provide a status of expire. All the certificates certainly cannot be edited but there is a lot of reasons to be revocable, for instance the case of mistake or the existence of a fraud later. Every time you issue a certificate, there is an output, a little bit of coin that remains in the issuer's account and by spending that output it will revoke the certificate and so anyone that tries to use that certificate, when someone tries to verify it, it will comes back with the status of revoked because is immutable.

Chapter 4

Conclusion

This chapter summarizes the results of this thesis and suggests potential extensions for our application and future work that could be arise exploiting the blockchain technology in fields of value and redefining the meaning of trust.

4.1 Summary of results

Latest technologies are enabling us to trust unknown people, companies and ideas, for instance social media, Airbnb, Uber and at the same time, trust in institutions and almost in every intermediary is collapsing. Thus, when a platform mediates, creates a new way of trust as well they are open to adopt new technologies such as Blockchain. At the same time Satoshi Nakamoto describes that trust could be replaced through cryptographic proof [1]. As Antonopoulos points out, blockchain is a network of assurance where trust is something computational, so can support more than just financial transactions, and that is more than an incentive to implement different applications [12].

After the completion of this thesis and taking into account the theoretical background and the previous work, we realize that our initial goal to provide a blockchain-based solution which could integrate into University is attainable. Although, our priority is to secure students' records, once the proposed application is implemented, it would affect a broader category that includes academic institutions, universities, corporate entities and hiring consultants.

The advantages are:

- Minimize of time process of authenticating academic certificates
- Elimination of fraudulent certificates
- No additional issuance fees
- Recipients are allowed to demonstrate ownership of their digital records
- The act of sharing certificates may be just a link
- Immediate verifications from employers
- GDPR compliant

4.2 Future work

This subsection explores the future work that needs to be done both in theoretical and practical level.

In particular, a similar application with various type of Blockchain, such as Ethereum or Hyperledger, could be tried in order to examine which are the differences and what is the prevailing one. This process could be also useful as a way to provide added secure.

If our use case for our Department would be tested in practice, it will be a first step to improve the current situation with the delivery of certificates and probably, if we reach to be in the map with the Universities which utilizes blockchain, it would a great chance for the University of Thessaly.

To sum up, based on the challenges presented in the literature review, we would like to propose research questions that need to be addressed to inform, for instance, how the public sector should approach the blockchain technology adoption.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, Available: https://bitcoin.org/bitcoin.pdf [Accessed July 1, 2018].

[2] M. Chung and J. Kim, "The Internet Information and Technology Research Directions based on the Fourth Industrial Revolution," *KSII Transactions on Internet and Information Systems*, vol.10 , no.3, pp.1311-1320, 2016, DOI: 10.3837/tiis.2016.03.020.

[3] M. Iansiti and K. Lakhani, "The truth about blockchain," *Harvard Business Review*, vol.95, pp.118-127, 2017, Available: https://hbr.org/2017/01/the-truth-about-blockchain [Accessed July 1, 2018].

[4] A. Gaggioli, "Blockchain Technology: Living in a Decentralized Everything," *Cyberpsychology, Behavior, and Social Networking*, vol.21, no.1, pp.65-66, 2018, DOI: 10.1089/cyber.2017.29097.csi.

[5] C. Fei, J. Lohkamp, E. Rusu, K. Szawan, K. Wagner, and N. Wittenberg, "Jolocom: Decentralization By Design," 2018, Available: https://bit.ly/2tJMPci [Accessed July 1, 2018].

[6] S. Kolvenbach, R. Ruland, W. Gräther, and W. Prinz, "Blockchain 4 Education," in *Proceedings of 16th European Conference on Computer-Supported Cooperative Work-Demos and Posters, Reports of the European Society for Socially Embedded Technologies, June, 4-8, 2018, Nancy, France*, DOI:10.18420/ecscw2018_p7.

[7] Blockcerts, Available: https://www.blockcerts.org [Accessed July 1, 2018].

[8] J. L. Zhao, S. Fan, and J. Yan, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue," vol.28, no.2, 2016, DOI: https://doi.org/10.1186/s40854-016-0049-2.

[9] Wikipedia, "Blockchain," Available: https://en.wikipedia.org/wiki/Blockchain [Accesed July 1, 2018].

[10] M. Peck, "Blockchains: How They Work and Why They'll Change the World," *IEEE Spectrum*, 2017, Available: https://bit.ly/2MEsgVB [Accesed July 1, 2018].

[11] Bitcoin Wiki, Available: https://en.bitcoinwiki.org/wiki/Blockchain [Accessed July 1, 2018].

[12] A. Antonopoulos, *Mastering* Bitcoin, Sebastopol, CA: O'Reilly Media Inc., 2015.

[13] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in 2017 IEEE International Congress on Big Data (BigData Congress), 2017, DOI: 10.1109/BigDataCongress.2017.85.

[14] Wikipedia, "Proof-of-work system," Available: https://bit.ly/2KUzOX5 [Accessed July 1, 2018].

[15] Digiconomist, "Bitcoin Energy Consumption Index," Available: https://digiconomist.net/bitcoin-energy-consumption [Accessed July 1, 2018].

[16] Medium, "Certificates, Reputation, and the Blockchain," Available: https://bit.ly/1T6OdO3 [Accessed July 1, 2018].

[17] Learning Machine, Available: https://www.learningmachine.com/ [Accessed July 1, 2018].

[18] UNIC, "Digitalcurrency," Available: https://bit.ly/2I5G3mj [Accessed July 1, 2018].

[19] CareerBuilder, Available: https://www.careerbuilder.com [Accessed July 1, 2018].

[20] Gradbase, Available: https://gradba.se [Accessed July 1, 2018].

[21] N. V. Patel, "Malta Pilots Blockchain-Based Credentials Program," *IEEE Spectrum*, 2018, Available: https://bit.ly/2NiaVTF [Accessed July 1, 2018].

[22] Wikipedia, "MIT License," Available: https://en.wikipedia.org/wiki/MIT_License [Accessed July 1, 2018].

[23] Bitcoin wiki, "SHA-256", Available: https://en.bitcoin.it/wiki/SHA-256 [Accessed July 1, 2018].

[24] R. Botsman, *Who Can You Trust? : How Technology Brought Us Together - and Why It Could Drive Us Apart*,Public Affairs, 2017.

[25] Medium, "The EU General Data Protection Regulation and the Blockchain", Available: https://medium.com/learning-machine-blog/the-eu-general-data-protection-regulation-and-the-blockchain-1f1d20d24951 [Accessed July 1, 2018].