



Umm Alqura University

College of Computers and Information System

Joint MSc in Computer Engineering and Science

**Issuing Digital Certificates Based on The Blockchain Technology**

**Master Thesis by :**

**Elham Abdullah Alsofyani**

**Thesis Supervisor by:**

**Dr. Khaled Tarmissi**

## **Abstract**

Digital transformation is considered as a fundamental stage toward electronic governance worldwide. The government sectors in Saudi Arabia seek to digitalize all their services. Therefore, providing electronic services has become one of the institutions' requirements to achieve the optimum levels determined by the digital maturity index in the kingdom.

Educational institutions have invested in this trend to develop many of their electronic services. Even though, educational certificates are still issued on paper in most of educational institutes. Paper certificates may increase validation obstacles. In addition to the possibility of fraud.

Blockchain technology is a promising revolution that used in a lot of fields. This technology offers several advantages that make it applicable in regard of electronic educational certificates. These advantages include decentralization, transparency and stability.

The aim of this thesis is to conduct an analytical study system for issuing digital certificates based on the blockchain technology. A model for an educational institution's certification were chosen. Then, the necessary changes of the ecosystem parts were made to be complied with certificate sample. Thereafter, the transaction was issued in the Bitcoin testnet that is available for developers for testing purposes.

The experiment of the system performance showed a noticeable efficiency in maintaining the integrity of the certificate contents. The issues related to the security and privacy of the system were discussed. As well as the suggestions for further development in this area.

## ملخص الرسالة:

يعتبر التحول الرقمي مرحلة أساسية نحو الحكومة الإلكترونية في جميع أنحاء العالم. تسعى القطاعات الحكومية في المملكة العربية السعودية إلى رقمنة جميع خدماتها. لذلك، أصبح تقديم الخدمات الإلكترونية أحد متطلبات المؤسسات لتحقيق المستويات المثلى التي يحددها مؤشر النضج الرقمي في المملكة.

استثمرت المؤسسات التعليمية في هذا الاتجاه لتطوير العديد من خدماتها الإلكترونية. على الرغم من ذلك، لا تزال الشهادات التعليمية تصدر على الورق في معظم المعاهد التعليمية. الشهادات الورقية قد تزيد من عقبات التحقق من صحتها. بالإضافة إلى إمكانية الاحتيال.

تعتبر تقنية البلوكتشين ثورة واعدة تستخدم في العديد من المجالات. تقدم هذه التكنولوجيا العديد من المزايا التي تجعلها قابلة للتطبيق فيما يتعلق بالشهادات التعليمية الإلكترونية. وتشمل هذه المزايا اللامركزية والشفافية والاستقرار.

الهدف من هذه الأطروحة هو إجراء دراسة تحليلية لنظام إصدار الشهادات الرقمية على أساس تكنولوجيا البلوكتشين. تم اختيار نموذج لشهادة مؤسسة تعليمية. بعد ذلك، تم إجراء التغييرات اللازمة لأجزاء النظام الإيكولوجي للامتثال لعينة الشهادة. لاحقاً، تم إصدار المعاملة البيئية التجريبية لشبكة البتكوين المتاحة للمطورين لأغراض الاختبار. في

أظهرت تجربة أداء النظام كفاءة ملحوظة في الحفاظ على سلامة محتويات الشهادة. تمت مناقشة المشكلات المتعلقة بأمان وخصوصية النظام. وكذلك الاقتراحات لمزيد من التطوير في هذا المجال.

## **Acknowledgments**

At first, I thank Allah Almighty, who enabled me to write this thesis.

Special thanks to the supervisor of this thesis Dr. Khaled Al-Tarmissi for his great efforts and valuable guidance's throughout the research phase.

All thanks and gratitude my parents, my family and everyone who supported me and encouragement for completing my educational career.

## Contents

<b>Abstract</b> .....	II
<b>Acknowledgments</b> .....	IV
<b>List of Figures</b> .....	VII
<b>List of Table</b> .....	VIII
<b>CHAPTER 1: Introduction</b> .....	1
<b>1.1 Motivation</b> .....	1
<b>1.2 Purpose and research questions</b> .....	2
<b>1.3 Limitations</b> .....	3
<b>1.4 Literature Review</b> .....	3
<b>CHAPTER 2: Technical Background</b> .....	7
<b>2.1 Blockchain and Cryptocurrency:</b> .....	7
2.1.1 Bitcoin:.....	8
2.1.2 Ethereum: .....	9
<b>2.2 Cryptography:</b> .....	10
2.2.1 Symmetric Algorithms: .....	10
2.2.2 Asymmetric Algorithms or (or Public-Key) Algorithms:.....	11
2.2.4 Hash functions:.....	12
2.2.4 Merkle tree:.....	13
2.2.5 Digital Signature:.....	14
<b>2.3 Blockchain Layers:</b> .....	16
2.3.1 Data layer: .....	17
2.3.2 Network layer:.....	18
2.2.3 Application layer: .....	19
<b>2.4 Types of Blockchain</b> .....	22
<b>2.5 Advantages blockchain:</b> .....	23
<b>2.6 Applications of Blockchain:</b> .....	24
<b>CHAPTER 3: Methodology</b> .....	28

<b>3.1 Design Certificate schema .....</b>	<b>29</b>
<b>3.2 Issuing Certificates .....</b>	<b>33</b>
<b>3.3 Develop Certificate viewer .....</b>	<b>37</b>
<b>CHAPTER 4: Verification and Evaluation .....</b>	<b>43</b>
<b>4.1 Verification Process: .....</b>	<b>43</b>
<b>4.2 Evaluation of security requirements .....</b>	<b>46</b>
<b>4.3 Evaluation of privacy requirement .....</b>	<b>50</b>
<b>CHAPTER 5: Conclusion .....</b>	<b>51</b>
<b>5.1 Discussion Results: .....</b>	<b>51</b>
<b>5.2 Future work: .....</b>	<b>51</b>
<b>References .....</b>	<b>53</b>

## List of Figures

Figure 2.1 : The Blockchain Data Structure.....	8
Figure 2.2 : Symmetric Cryptography .....	11
Figure 2.3 Asymmetric Cryptography .....	12
Figure 2.4 : Merkle tree representation .....	13
Figure 2.5 : Digital Signature Process.....	14
Figure 2.6 : Blockchain Layers.....	16
Figure 2.7 : Block structure in Bitcoin .....	17
Figure 2.8 : peer to peer system .....	18
Figure 3.1: Issuing process.....	29
Figure 3.2 : Certificate form .....	29
Figure 3.3 : running create_certificate_template script .....	33
Figure 3.4 : running instantiate_certificate_batch script.....	33
Figure 3.5 : JSON files for each recipient.....	33
<i>Figure 3.6 : bitaddress.org website .....</i>	<i>34</i>
<i>Figure 3.7 : the faucet testnet that was used .....</i>	<i>35</i>
Figure 3.8 : Blockchain Explorer .....	36
Figure 3.9 : Home page with basic configuration .....	38
Figure 3.10 : The web page that displays the certificate data .....	39
Figure 3.11 : webpage form to request certificate .....	40
Figure 3.12 : Bitcoin keys webpage .....	41
Figure 3.13 : message request confirmation.....	42
Figure 4.1 : anchors filed.....	43
Figure 4.2 : signature fields .....	45

## List of Table

Table 3.1 : Programs and tools that were used .....	28
Table 3.2 : shows the global fields that are used to create the certificate template .....	31
Table 3.3 : The additional fields for each recipient .....	32
Table 3.4: shows the data for students .....	32
Table 3.5 : content of file local.ini .....	37
Table 4.1 : Result of validation process after modification .....	47
Table 4.2 : Image and value of encoding to Base64 .....	48



## CHAPTER 1: Introduction

### 1.1 Motivation

The scientific certificates are valuable documents in the life of any person. It determines the level of education and qualification for the future job. The institutions make efforts to ensure the validity and integrity of these qualifications and certificates. As the educational institutions increases around the world, assurance of the certificates has become a concern of the educational institutions and employment agencies. The digital certificates are a major development in terms of the speed of issuance, distribution and give permissions to the relevant parties to access. This facilitates the admission process to universities and jobs, saves costs and reduces the possibility of manipulation and modification of these sensitive documents.

Many of educational institutions still rely on the issuance of hard copy certificates. Those documents contain security features that prevent fraud. However, the cost of materials, human efforts of issuance, distribution and follow-up remains high, and the risk of fraud remains with the great technical development.

In the Kingdom of Saudi Arabia, some educational institutions were started to provide data for certificates electronically. The noor system that initiated by the ministry of education is an example. This system issues certificates for the all levels of schools and provide some data of secondary school certificates to the local universities and colleges. So, the students do not need to provide a hard copy of their certificate when they apply for any college. This system makes the admission process easier. Nevertheless, centralization in this system is an obstacle, as linking all educational systems and employment parties is very difficult.

For blockchain technology, transactions are broadcast. Every node is creating their own updated version of events. Which provide immutability, transparency, and trustworthiness for all transactions executed on a blockchain network. This difference makes blockchain technology so useful. It represents an innovation in information registration and distribution that eliminates the need for a trusted additional party to facilitate digital relationships.

Blockchain "is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data"[1]. It proposed by Satoshi Nakamoto in 2008 [2]. There are many areas where Blockchain Technology can be applied Such as health, education, commerce, etc. Blockchain technology has many advantages that make it applicable in the field of education, especially the issuance of educational certificates such as: decentralization traceability and immutability [2].

Hence the importance of this master's thesis in providing secure digital education certificates to preserve documents from alterations, simplify the procedures, reduce the material cost and save time and human effort.

## **1.2 Purpose and research questions**

The goal of this master's thesis is to demonstrate how blockchain technology can be used to provide a mechanism for validating digital certificates. The research goal can be broken down into two research questions:

- First Research Question:  
How the project can be applied to a different sample of educational certificates?

This question will be answered in Chapter 3. By showing how the certificate schema is designed, released, and displayed

- Second Research Question:

How the system meets security and privacy requirements?

The answer to this research question will be answered in Chapter 4.

Where security and privacy criteria will be determined to evaluate the system

### **1.3 Limitations**

The project consists of a set of tools, mobile applications, and open source libraries that serve as a system for the design, certification and verification of issued certificates.

The research was limited to using the main libraries that allow us to conduct the experiment. These libraries are: cert-tools, cert-issuer and cert-viewer. The transaction has been published to the testnet for Bitcoin.

For the certificate viewer cert-viewer was used to view and verify certificates. It is Python Flask app.

### **1.4 Literature Review**

Blockchain technology attracted the attention of many researchers. Many of this research were focused on the Bitcoin system. Others focused on other applications such as smart contracts[3]. So, published scientific research on the applications of blockchain technology in the field of education are increasing significantly. Especially in respect of digital certificates.

An article published in 2018 about Exploring blockchain technology and its potential applications for education [2]. This article highlights the Digital Certificates Project as an important application for blockchain technology in the educational field. This project builds an ecosystem for creating, sharing, and verifying blockchain-based educational certificate[4].

Sharples et al published an article titled (The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward) This article discusses the possibility of applying blockchain technology in the field of education. The researchers discussed the application of this technology and its impact in three areas. First: The blockchain as a Distributed Digital Record: An obvious educational use is to store records of achievement, such as degree certificates. Second: The blockchain as a Proof of Intellectual Work. Finally, The Blockchain as Intellectual Currency [5].

Another article discussed the blockchain usage in education. The researchers presented a detailed explanation of technology and its use in education generally. The use of this technique for the issuance of educational certificates. This study concluded that the reliance on blockchain technology for to issue certificate will produce an immutable digital certificate which are valid for perpetuity. [6]

Zyskindand et al described a decentralized personal data management system. This system permits users to own and control their data. They implemented a blockchain based protocol that using an automated access-control manager thus did not require a trusted third party. The study indicated the impact of applying technology to organizations as well. As their role would be limited to using the data correctly without worrying about its storage[7].

Bandara et al explained the model of granting apprenticeship degree based on blockchain technique. The effectiveness of the model will create an institutional trust. As well as the great impact on employers and its applicability to different educational institutions. The apprenticeship degree data are stored in the decentralized book of accounts in a secured database. This database can be shared, copied and synchronized for validation[8].

Another article presented the architecture of the Disciplina platform. The researchers described the architecture for storing the educational records in the blockchain. Privacy of these records are preserved. The blockchain technology used in this project allows to create a trusted and validated digital curriculum vitae for any person[9].

Turkanovic et al are proposed a platform for the classification of higher education certificates. It will convert the higher education system from traditional records to a decentralized and secured system based on blockchain technology[10].

Cheng et al developed a decentralized application and designed a certificate system based on Ethereum blockchain. In this study Description of the proposed system To issue and verification certificates [11].

In " Better Security Over Blockcerts" the system is designed to improve several aspects in a project released by the Massachusetts Institute of Technology's Media Lab. By using a multi-signature scheme to issue certificates. And use a secure mechanism to revoke certificates. In addition to establishing a secure federal identity to confirm the identity of the issuing institution [12].

Ocheja et al made the first practical application of the platform based on blockchain to track learning achievements. Where smart contracts were used to manage operations within this platform. The BOLL system allows learners to transfer learning records from one institution to another securely. The BOOL system also ensures continuity of data in previous learning stages[13].

Choi et al present system gives learners badges to evaluate the learning process. The system collects and displays badges obtained in a storage

environment called a backpack. This system is compatible with the Open Badges of IMS Global Learning Consortium The badge is validated through the blockchain network[14].

The Open University project offers a decentralized platform. This platform uses blockchain to validate the credentials of learners. it also use smart contracts to provide jobs tailored to learners' skills. Matching algorithms facilitate the HR function and reduce recruitment costs. The platform also provides academic analysis that enables learners to communicate with educational services providers and gathering in alumni networks[15].

## CHAPTER 2: Technical Background

### 2.1 Blockchain and Cryptocurrency:

Financial transactions are one of the most important transactions in daily life. In the past, it was based on barter and exchange of goods. But it was found that this method does not fit the needs of most people. Therefore, countries have started using coins. Where People appreciate value of metals like gold and silver. Although metal pieces were easier to carry and better met the needs of the people than the previous regime, they were vulnerable to theft. Hence the idea of central banks as reliable parties. Whereas the basis for the stability of any financial system is trust.

In the early nineties and with the expansion of the use of the Internet, banks moved to establish digital systems to facilitate operations. where financial balances are digitally stored in the systems.

Electronic commerce depends on reliable centralized outsiders. The actual design of the Internet is a peer-to-peer network. However, the lack of maturity of the technology and the need for trust then prompted people to build up centralized systems. The significant growth in the number of transactions demonstrated the defects of the central systems, such as the high cost of transactions and the time to settle the deal. Consequently, cryptocurrencies were appeared. Cryptocurrencies can be defined as " digital assets designed as electronic money that uses encryption techniques to ensure the security of funds and transactions." [17] The first cryptocurrency, bitcoin, appeared in 2008 as one of the applications of blockchain technology and it has the same advantages of blockchain technology . [16]

The blockchain can be defined as a "set of ordered blocks of data. Each block contains several verified transactions and usually contains a pointer to the previous block in the chain. This, together with the fact that

copies of each block are stored on multiple nodes in the network, ensures that no one user can modify the contents of any block without other users detecting it. In most cases, to have any chance to successfully make a malicious transaction, one user has control more than 50% of the network. This creates a trusted environment where the architecture of the system itself plays the role of a trusted medium [19]". Figure 2:1 shows the structure of the blockchain data.

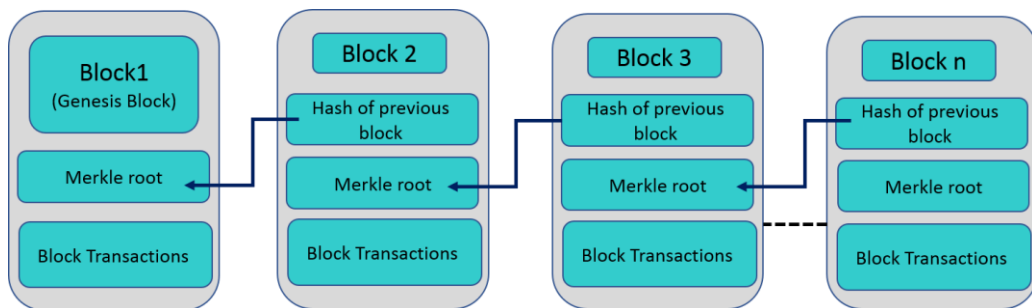


Figure 0.1 : The Blockchain Data Structur

There are over 60 cryptocurrencies from which it can be described as a major depending on the network structure and the number of users and other currencies that can be exchanged for it.[18]. The project that used in this research provides the possibility to use Bitcoin or Ethereum cryptocurrency.

### 2.1.1 Bitcoin:

The Bitcoin currency was presented in the research paper [16] as an electronic monetary system based in financial dealings on a peer-to-peer principle. Bitcoin is one of the cryptocurrencies and is the first of its kind and the most widespread and famous. Also, many of cryptocurrencies currently adopt the same principle of Bitcoin. Bitcoin holds a value with eight decimal places of precision. The smallest value in Bitcoin is 0.00000001 and is called 1 Satoshi. It has no categories like traditional



currencies. Mining operations continue to confirm the validity of deals and the production of new formation currencies to reach the maximum limit of 21 million coins after that, it is not possible to issue currencies with new configuration and the circulation will be used only. The price of bitcoin is experiencing great fluctuations due to several factors, including supply and demand and currency trading in several countries, which leads to a difference in the exchange rate.

Considering Bitcoin currency as a blockchain application, the organization of data in a block and the method of linking blocks It will be mentioned in Data layer section. Bitcoin uses a proof of work (POW) algorithm to achieve consensus and add new blocks to the chain [17].

#### 2.1.2 Ethereum:

Blockchain technology is not only used for financial transactions, there are many uses. Ethereum provides a standard for building different blockchain-based applications. Ethereum uses an abstract base layer that hides the complexities of software from developers and allows them to build decentralized applications that use the same strings instead of creating different strings for each application. Commonly, scripts written in Solidity are called smart contracts. Smart contracts are like contracts in the real world and are programming instructions that are managed and implemented between the parties through the blockchain network. When publishing transactions, the mining process is carried out by the miners in the network, and (Ether) is paid as transaction fees to ensure the continuity of the system and to limit the publication of insignificant transactions. Ethereum data structure is very similar to bitcoin, except that there is a lot of information in the block header and use Patricia trees are a form of Radix trees that facilitates efficient insert/delete operations.[16]

## 2.2 Cryptography:

The interest in cryptography is increasing as a part of technical development which has become essential for daily electronic dealings [18]. Where the cryptograph is an essential process to secure the important data within the network. According this Several techniques are used for encrypting the information in blockchain technology. Cryptography involves two basic processes:

"– Encryption: Encryption is a process of converting your message into code so that only authorized parties can access it.

– Decryption: Decryption is reversing the encryption process so that the message can be converted to the original message." [17]

Cryptography is divided into three main branches: Symmetric Algorithms, Asymmetric Algorithms or (or Public-Key) Algorithms and Cryptographic Protocols. [18]

### 2.2.1 Symmetric Algorithms:

The symmetric algorithms are also known as conventional algorithms or single-key algorithms. The plain text encryption is done by using the encryption algorithm. This encryption algorithm receives plain text and secret key as input. The secret key value is an independent value of plain text. Then, the encryption algorithm makes changes in the plain text based on the value of the secret key to get the encrypted text which is incomprehensible. The encryption algorithm makes changes to plain text using two methods:

- Substitution: Any element, character, bit, or bit set in the original is replaced by another element
- Transposition: This is where the original text elements are rearranged

In both methods, no data should be lost.

The decryption process is done using the decryption algorithm, which is the inverse algorithm of the encryption algorithm. The decryption algorithm receives the private secret key and encrypted text as input and produces the plain text again.

Figure 2:2 shows the encryption process using symmetric algorithms.

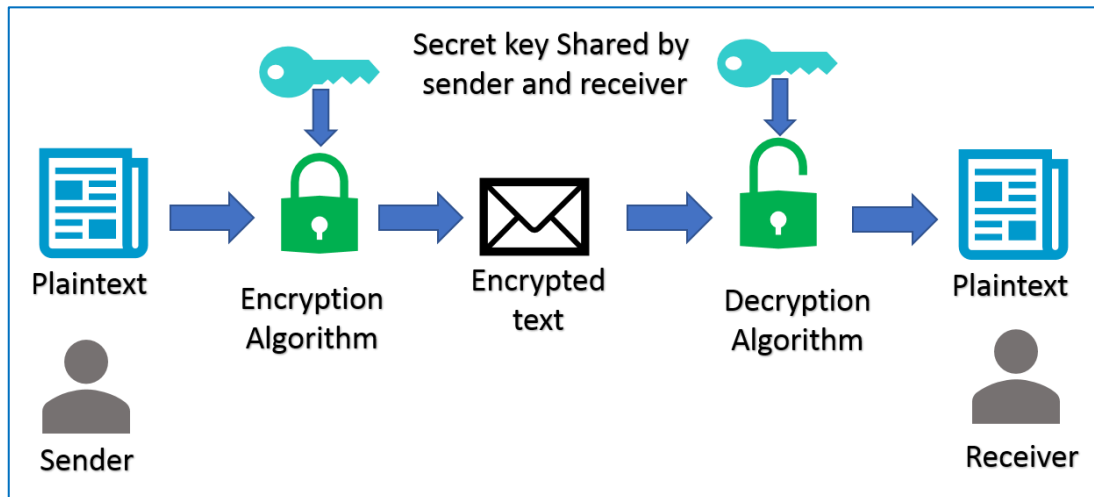


Figure 0.2 : Symmetric Cryptography

### 2.2.2 Asymmetric Algorithms or (or Public-Key) Algorithms:

Unlike the symmetric encryption that use only a single secret key shared between the sender and receiver. Two types of keys are used in asymmetric algorithm. Both the sender and receiver have a pair of keys: a public key which distributed freely between users for encryption, and a private key which keep confidential for decryption purposes.

Asymmetric encryption is commonly used either in public key encryption or in the digital signature. The main aim of using public key encryption is to maintain the message confidentiality. In this case, the sender uses the receiver's public key to encrypt the message and the receiver can decrypt the message using its own key. While the purpose of using a digital signature is (authentication) to ensure that the sender created the message in

addition to verifying the integrity of the message. In this case the sender uses the private key to sign the message and the receiver uses the sender's public key to validate the signature [19]. Figure 2.3 illustrates asymmetric cryptography.

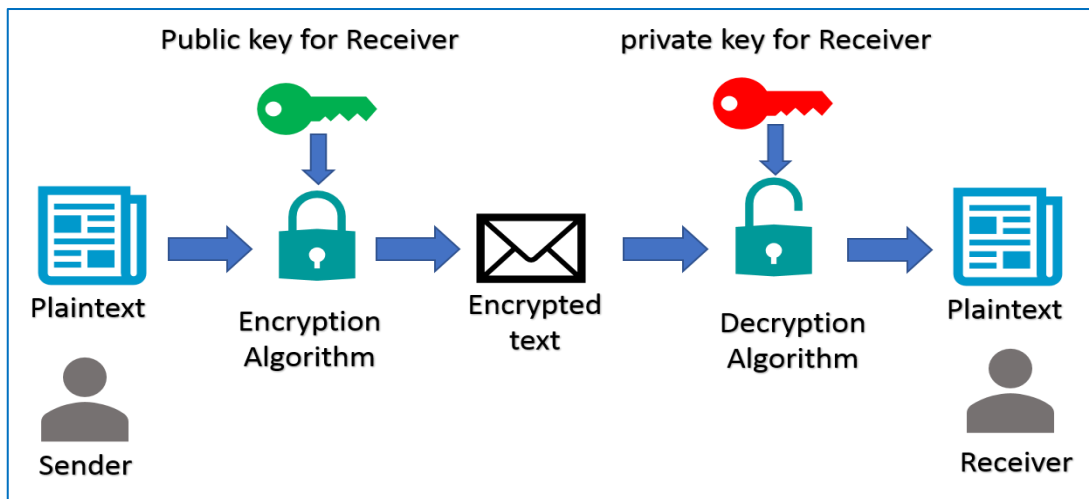


Figure 0.3 Asymmetric Cryptography

#### 2.2.4 Hash functions:

The hash functions are one of the encryption techniques which defined as "a one-way function that converts input data of arbitrary length and produces a fixed-length output. The output is usually termed "hash value" or "message digest." " [16]. For hash functions to achieve the purpose of their design, they must be characterized by the following:

- The input chain can be of any size while the output is of fixed length.
- We get the same hash value if the same input is provided for the same hash function.
- The original data cannot be obtained from the same hash value.
- Any slight change in the value of the input data significantly affects the resulting hash value.

Based on the above, the value of the hash function is a unique imprint of data. It can compare data and detect any change in it. Hash references can

also be used to store data in a sensitive manner. This can be achieved by utilizing either the chain model used to build the chain blocks, or by the tree model which stores transaction logs such as in a Merkle tree.[20]

### 2.2.4 Merkle tree:

A Merkle tree is a "binary tree of cryptographic hash pointers, hence it is a binary hash tree[16]". It is a form of data structure in which hash values are stored in a hierarchy that is tamper-resistant and ensures the ordering of transactions.

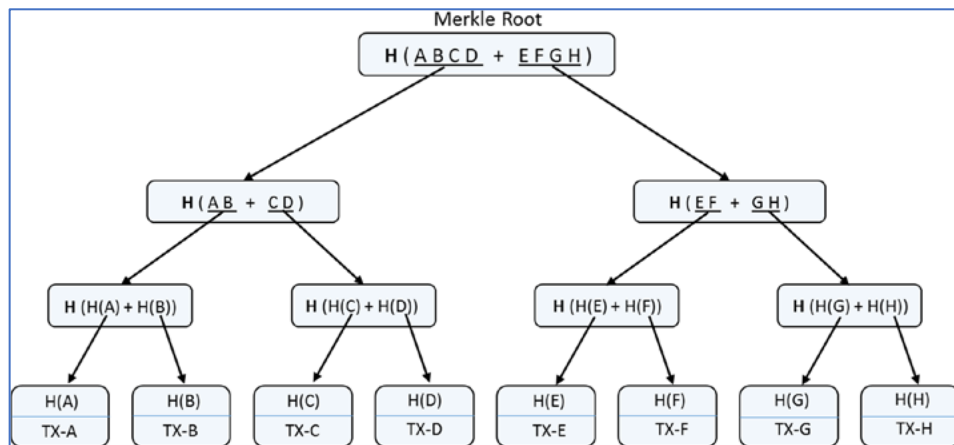


Figure 0.4 : Merkle tree representation

Figure 2.4 represents the storage and hash values of transactions in a Merkle tree model. For instance, the value TX-A stands for a transaction data block. While the value H(A) represents the hash value for the same transaction.

All hash values are aggregated in pairs at the next level. This aggregation of the hash values is repeated until a single hash reference is reached. This hash reference is called the Merkle root. This Merkle root is stored in the block head and is used to validate the transaction.

### 2.2.5 Digital Signature:

In the real world, the traditional handwritten signature is used to prove that someone has created a message such as signing a contract or signing a check. There are legal consequences that prevent most people from attempting to forge a signature.

In the field of digital transactions, digital signature is used to achieve the same goal. The digital signature uses encryption algorithms so that only the sending person can create a valid signature.[18]

The hash values are a unique fingerprint of data. Fixed length of hash values is used for any data size. Therefore, this encryption technique is appropriate for using in the digital signature process. The signature algorithm and the verification algorithm deal with distinct message values along with a fixed length.

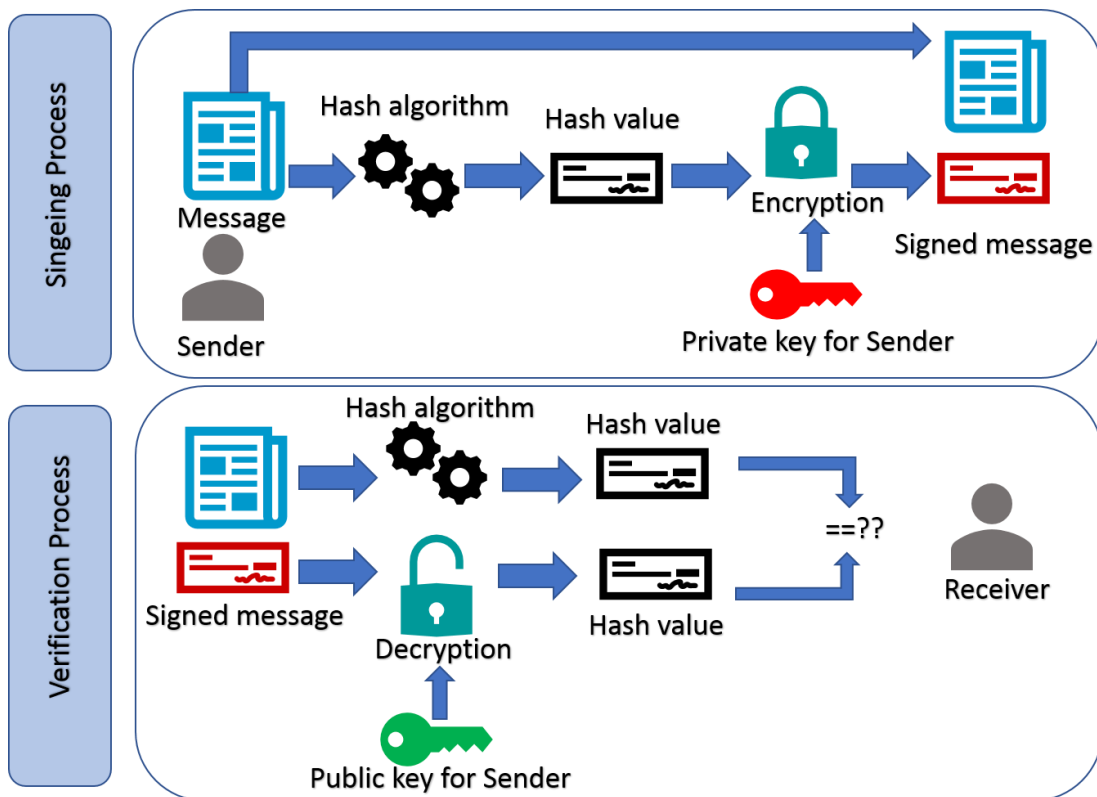


Figure 0.5 : Digital Signature Process

As shown in the figure 2:5, the digital signature process starts by calculating the hash value of the sent message  $h$ . The hash value is then encrypted using the sender's private key and sent with the message to the receiver.

Signature validation is done by decrypting the hash value using the sender's public key and thus obtaining the hash value  $h'$ . The hash value of the original message is calculated, and the two values are compared. If both values are equal  $h=h'$ , the message is integrated, and the digital signature is correct.[21]

Digital signature schemes consist of three main elements:

- A key-generation algorithm that generates two keys, one is public and shareable. While the other one is private and confidential.
- The signature algorithm is used to produce the signature of the approved message using the private key.
- The verification algorithm receives the message and signature as input and uses the public key to validate the signature.[22]

Digital Signature offers the following security services:

- The confidentiality of data is maintained. Only authorized persons have the access for this data.
- The integrity is ensured. Messages were not modified during transmission.
- Facilitate the authentication of both sender and data origin. Which ensure the message is sent by the permitted sender only.
- Nonrepudiation: The sender of a message cannot deny the creation of the message.[18]

There are several ways to enforce the authenticity of a key[19]:

– Public Key Infrastructure (PKI): It contain a set of policies, processes, programs and platforms that used to issue, maintain, and revoke public key

certificates and to manage public and private key pairs such as Certificate Authorities.[23] This method is most commonly used.[18]

– Web of Trust, Key ownership is asserted by individuals in a decentralized environment.[19]

– Domain Name System (DNS) : "It is a directory lookup service that provides a mapping between the name of a host on the Internet and its numerical address. [23]" can be used to look up and verify the signed message.[19]

### 2.3 Blockchain Layers:

Blockchain is a complex technology. It is a combination of working principles related to computer science, encryption and economics. Therefore, the blockchain technology can be divided into several layers to provide a better understanding of this technology and to facilitate the construction and maintenance of application[16]. These layers are the application layer, the data layer, and the network layer as shown in figure 2.6 [24].

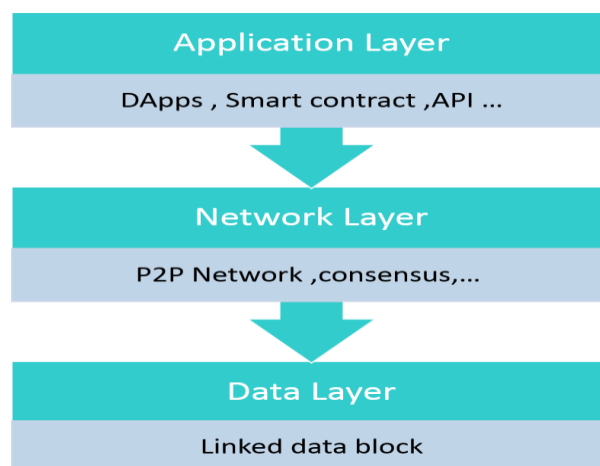


Figure 0.6 : Blockchain Layers



### 2.3.1 Data layer:

It contains a series of Linked blocks. Each block in the chain consists of a header and body. The block header includes the following data: version, Previous Block Hash, Merkle Root, Timestamp, Difficulty Target and Nonce. While the body of block contains Transaction Counter and Transaction List[16]. Figure 2.7 show Block structure in bitcoin.

Head of Block	Block identifier	4 bytes
	Next block identifier	4 bytes
	Block size	4 bytes
	Block version	4 bytes
	Previous block hash	32 bytes
	Block Merkle root	64 bytes
	Block timestamp	8 bytes
	Nonce	4 bytes
Body of Block	Transaction counter	4 bytes
	Transaction list	1 MB

Figure 0.7 : Block structure in Bitcoin

Transactions are the basic data in the blockchain, including input (sender details), output (recipient details) and digital Signature[25].

### 2.3.2 Network layer:

Principally, the computers or servers connected to the network are called peers or nodes. Those peers or nodes communicate with each other on the Internet via a peer to peer (P2P) network. This network defined as: "A type of computer network that uses a distributed architecture. Each peer or node shares the workload and is equal to the other peers, meaning there should not be any privileged peer". P2P demonstration is shown in figure 2.8. Therefore, the blockchain is a peer-to-peer transaction system without a reliable third party.

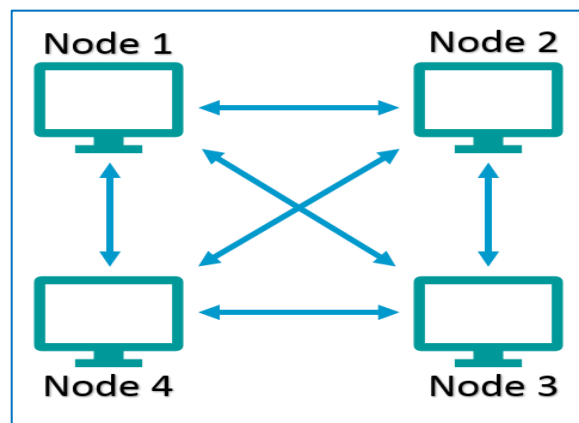


Figure 0.8 : peer to peer system

### Consensus Algorithms:

A peer-to-peer network uses consensus algorithms. Consensus algorithms are essential in blockchain systems. The purpose of these algorithms is to reach an agreement between the different nodes. Hence, the security and integrity of the blockchain are preserved. There are different methods to achieve compatibility between nodes. Those methods include PoW (Proof of work), PoS (Proof of stake), PBFT (Practical byzantine fault tolerance), DPOS (Delegated proof of stake). Ripple and Tendermint[16]. PoW (Proof of work) will explained as an on of the protocols that used in bitcoin network.

### Proof of work (PoW):

This algorithm is used in the Bitcoin's and Ethereum's transactions as well as other blockchain's applications. It designed to provide a secure and trustful environment. Basically, the nodes that calculate the hash value are called miners. While the process of calculating the hash value of the new block is called mining. Each block contains block header, which includes the hash value of the previous blocks in addition to other dataset .

The miners try to calculate the hash value of the new block by changing a value of nonce. In this way, the computer resources of the participating nodes are exploited to solve this mathematical puzzle. In fact, there is no specific algorithm can be used to find out the hash value. A competition existed to find out the right hash value .

When one node reaches its target value, it will deploy the block to the other nodes. The nodes perform a mutual confirmation of the validity of the new hash value, and then the block is added to the blockchain.

In public networks, reward provided to the first user who find out the target hash value of the transaction using his own resources. This will ensure the continuity of the system [27].

### 2.2.3 Application layer:

The application layer is consisting of distributed application (dApps) and smart contracts. The blockchain network communicates with applications via the Application Programming Interface (API) [26]. The API facilitate the link between the dApp and other products and services without needing to know implementation details.

In this layer the functions required for end users are programmed. It includes APIs, development frameworks, scripting etc.[16]. The application

layer provides a means for the customer to communicate with the network[17].

The application layer can be divided into two sub-layers, the application layer and the execution layer. The application layer represents the front end that the user sees. while the execution layer includes smart contracts that form entire business logic. A dApps is assumed as a web application that interacts with the chaincodes as well as smart contracts.[27]

### **2.3 Storing data in a blockchain**

The transaction data storage is one of the most important decisions related to the system designation based on blockchain. This decision depends on the field of use. In this section, all possible methodologies for storing data will be discussed.

In general, transaction data can be stored on chain or off chain. The first approach is to store data within the blockchain. The most important advantages related to this approach are the presence of multiple copies of data and decentralization. While the huge volume of data that can be stored is considered as one of the most prominent problems. The disadvantages of storing data within blockchain are the high cost as well as very limited storage capacity may reach 1 KB. Also, the data stored in the blockchain must be downloaded by the full Node and this justifies the high cost of storage and security concerns about disclosure of data.

According to the policies related to the security and management of confidential and sensitive data, some entities delete data after a period, and this cannot be done with the data stored in the blockchain according to the design.

The second approach is to store data fragmentation in a blockchain, while other raw data can be stored using any storage mechanisms. Many developers tend to use this approach to avoid the negative aspects of the previously mentioned approach. The value of the hash itself is stored in the blockchain.

In this method, the hash value of the transaction is used as an identifier. Thereby, data integrity will be ensured. The traditional storage methods will help in regard of inquiries for instance.

Several off-chain storage options can be used such as:

1- Traditional databases such as MySQL or MongoDB, which are characterized by strong query capabilities and low cost of storing large amounts of data. The downsides include centralization and loss of transparency.

2- Distributed databases where data is copied in many nodes and locations to avoid a single point of failure. This will lead to more capabilities to query as well as the low cost of storing data compared to the blockchain. One of the most prominent examples of these systems is MongoDB. The replication of data can be enabled, or the use of cloud storage solutions Like Azure CosmosDB. These systems still lack decentralization and loss of transparency.

3- Distributed File System: This system is similar to the distributed databases regarding the presence of multiple copies of data. But the file system does not have strong query capabilities. The file can be accessed through the file name and file path. Interplanetary File System (IPFS) is one of the most prominent distributed file systems that can be integrated with the blockchain network[28].

## 2.4 Types of Blockchain

Blockchain systems are classified into 3 types public blockchain, consortium blockchain and fully private blockchain.

1-Public blockchain: all records are visible to the public and everyone could take part in the consensus process. Public blockchain networks are immutability as it is very difficult to tamper with transactions. In terms of efficiency, the deployment of transactions takes a lot of time and blocks. So, public networks are characterized by limited productivity. In addition to the public blockchain is decentralized.

2-Consortium blockchain: The consortium blockchain constructed by several organizations is having elements of both public and private chains. A small portion of nodes would be selected to determine the consensus. The permission of reading the transactions could be public or restricted. The consortium blockchain can be tampered with transaction data. The number of validators may be more efficient than the public blockchain. The consortium blockchain is partially decentralized

3-Private blockchain: a group of pre-selected nodes would participate in the consensus process. only those nodes that come from one specific organization would be allowed to join the consensus process. A private blockchain is considered as a centralized network since it is fully controlled by one organization. It is fully controlled by one organization and the organization could determine the final consensus. Read permission for Transactions could be public or restricted. In private blockchain, it can be easily tampered with it as the number of participants is limited. They may be more efficient due to the small number of validators. The private blockchain is controlled by a one group and it is a fully centralized decentralized network.[27]

## 2.5 Advantages blockchain:

The blockchain architecture offers a lot of characteristics such as:

- 1) Decentralization: Transactions in traditional systems are validated by a trusted third party. This leads to higher cost and increased burden on central servers. While Block-matching algorithms are used to maintain data consistency in the distributed network.[27]
- 2) Transparency: Transaction data published on the blockchain network are open and reliable. Where each node has the same network access and query for authorized transactions according type of blockchain [31].
- 3) Persistency: Blockchain systems enable the detection of incorrect transactions. Also, it is difficult to delete or modify data once added [27]
- 4) Anonymity: Users interact with blockchain systems using the keys generated, without revealing the identity of the user. The system uses Asymmetric encryption in both data encryption and in digital signatures. This will ensure the transaction is not forged. Also, it guarantees the transactions were issued by the signatory without the need to reveal the user's identity.[27]
- 5) Traceability: The blockchain network uses time stamps to maintain order of transactions and to facilitate audit. Using a timestamp reduces the cost of data tracking and prevents data change after insertion. The transaction is recorded in the system after reaching a consensus of most of the node. Also, it is difficult for an attacker to manipulate data as it needs to control more than 51% nodes in the network.[31]
- 6) Credibility: Blockchain systems are highly credible through multiple ways. First, the usage of consensus algorithms to reach agreement on

a transaction before registration. Second, the encryption of transaction and binds the new block to the previous block. Finally, storing transactions across network devices instead of storing them on a single server. All these mechanisms will enhance the system credibility.[31]

## **2.6 Applications of Blockchain:**

Various categorization systems were used for blockchain applications. Those applications classified based on either blockchain versions or financial use for instance. However, categorization by field of use is the best way to include all the implementation of this technology.

Although this study tries to include all blockchain applications, this promising technology can expand and will not limit to the mentioned use in the coming future.

A systematic literature review published in 2018 to provide a classification for blockchain applications, current limitations, opportunities, and research gaps. 260 articles and 54 reports included between 2014 and 2018 in order to assess all applications for blockchain. Ten main scopes were determined as the following: Business and industry, finance, integrity verification, governance, IoT, health, privacy and security, education, data management, and miscellaneous.

The blockchain practices have some overlap and interrelations in most of the scopes. For example, finance-specific applications may include privacy and data management related applications. For practical categorization, thematic identification used to classify the blockchain fields. Blockchain applications in business and industry fields account for 22.6% of the total articles included in this literature review, followed by IoT and



governance implements which represent 12.5% and 11.3% respectively. The education implementations represent 3.1% of the total article, which is the lowest percentage among other field of use.

Blockchain technology is not suitable for all fields. This may consider a limitation for use. In some cases, blockchain will not have beneficial addition if no data need to be stored or one operator using the system for instance [29]

1) Financial applications:

Studies are still ongoing to find out the applied aspects of blockchain technology in the financial field such as payment and exchange of cryptocurrency (e-wallets), financial auditing, enabling global payments and currency exchange.

2) Integrity verification:

Integrity checking is one of the emerging blockchain applications. Where transaction and service information are stored in decentralized manner. These transactions cover several areas such as intellectual property, digital content, medical and educational records, and insurance.

3) Governance

Using of this technology may significantly change government business. There are many records and transactions that government agencies must manage. Given the advantages that this technology offers, it increases the efficiency of government operations and hinders corruption. It can be used for digital ID, passports and legal documents.

4) Internet of things

The interest is increasing in the Internet of Things as it has growing impact on many aspects of life. Blockchain technology can be used to

enhance its capabilities and providing a reliable and secure exchange of data. Especially in case of increasing the number of connected smart devices. Blockchain technology can increase the security of IoT and wireless sensor networks using the peer-to-peer decentralization network model.

5) Healthcare management:

In the field of health care, many applications that use blockchain technology have emerged. The most prominent one is the electronic patient healthcare records management systems that guarantee security and privacy.

6) Privacy and security:

Blockchain technology can enhance the security aspects of big data. It also enhances security and reliability in distributed networks using software and hardware solutions. Moreover, it enables the implementation of public key infrastructure and privacy platforms. As well, it is used to build protection systems against cyberattacks.

7) Business and industrial applications:

Blockchain technology can play a major role in changing business and industrial situations by automating business processes and improving credibility in e-commerce. It can also form a decentralized business management system for several organizations, which improves performance and reduces time and cost to complete operations.

Thus, sellers and buyers are able to deal directly without brokers' manipulation, as well as identifying counterfeit products and improving inventory management and performance

The potential applications of technology in the energy sector may have a significant impact as it will enhance transparency and confidence in

the energy market system. It can also be used as a framework for the issuance of bills and energy operations.

8) Education:

In the field of education, storing educational records and managing certificates is the most prominent use of blockchain technology. Smart contracts can be used to design pre-planned educational activities. It can also be applied to issue educational identities.

The digital currency can also be a driver for promoting learning and achievement[2].

9) Data management:

Applications based on blockchain technology improve data management and facilitate auditing. Various organizations using traditional ways for joint management. Although, they do not reach the optimum level of full interoperability between the parties. However, there are encouraging results showing that blockchain can be used as an infrastructure for managing the flow of operations across organizations. There are also suggested models for distributing big data based on this technology. Access control and authentication mechanisms can be used to ensure safety and privacy of the distributed data.

10)Miscellaneous applications:

There are many areas that cannot be included under any of the previous categories, such as the use of blockchain technology in social media and in the humanitarian sector and charitable work. [29]

### CHAPTER 3: Methodology

The following overview is demonstrating the implementation process and technologies used in this project. The selected certificate form and the steps that were performed to design, issue and view the certificate are presented.

The Digital Certification Project which named Blockcert developed by the Media Lab Learning Initiative and Learning Machine (MIT). The second version of the project was used .This project consists of three parts: cert-tools, cert-issuer, and cert-viewer.

First, the cert-tools is a command line tools for creating a template and batch of unsigned certificates. Second, the cert-issuer is a command line tools which include digital signature within the certificate file and publish the transaction on the bitcoin network. Finally, the cert-viewer is a python flask app for viewing and verifying certificates. These three parts form an integrated ecosystem for the issuance and presentation of digital certificates. Figure 3.1 showing Issuing process which include cert-tools and cert-issuer.

The table 3.1 displays the operating system, programs and tools which used to implement this experiment

program	type	version
Windows	Operating System	8.1
Python	Programing Language	3.6.4
Git Bash	command line Compatible with Windows	2.18.0
MongoDB	Database	3.6.3
Notepad++	Text editor	7.5.8

Table 0.1 : Programs and tools that were used

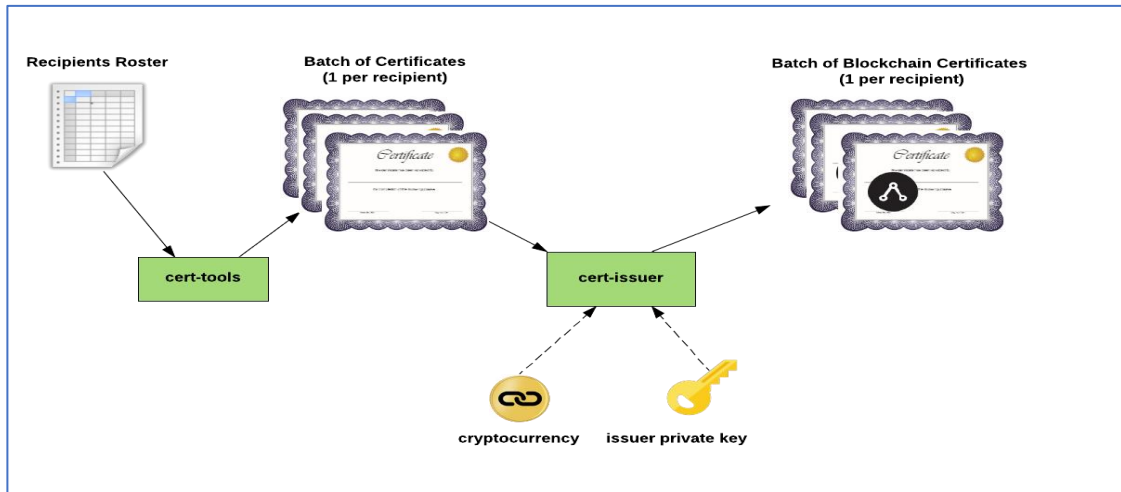


Figure 0.1: Issuing process

### 3.1 Design Certificate schema

The development of the certificate schema depends on the selected certificates in the Figure 3.2. The certificate contains the same data in Arabic and English language. The certificate schema will be designed using English language.



Figure 0.2 : Certificate form

The project is essentially based on the creation of file with JavaScript Object Notation data format, or JSON as abbreviation. JSON is a highly interoperable format for data interchange. It is a "textual representation defined by a small set of governing rules in which data is structured" [30]. According to JSON specifications, data can be represented as a collection of name/value pairs or an ordered list of values.

The design certificate schema phase can be divided into two steps. The first step is to design a certificate template, which contains global data that is repeated in all certificates such as the university name. The second step is to create a batch of certificates. In this step each recipient's data is added to certificate.

Initially the settings file will be edited. The settings file contains the global fields in the certificate template and defines the fields for each recipient. The table 3.1 shows the global fields that are changed to create the certificate template.

Type of fields	Field name	Value
issuer information	issuer_url	https://www.tu.edu.sa/
	issuer_email	websupport@tu.edu.sa
	issuer_name	Taif University
	issuer_signature_lines	{"fields": [{"job_title": "Dean of Admission and Registration", "signature_image": "images/issuer-signature.png", "name": "Dr.WASLALLAH ALSUWAT"}]}
	issuer_public_key	ecdsa-koblitz-pubkey: mhAFL5ov7skwaxb3wANXKnKNpTjoiaTSVr
certificate information	certificate_description	Hereby it is that The Council of Taif University in its fifth session has conferred upon in recogniion of fulfilment of the prescribed requirements of

Type of fields	Field name	Value
	criteria_narrative	,Student ID number ,National ID ,in recogniion of fulfilment of the prescribed requirements of ,The Degree of ,of ,From the College of ,With GPA of ,and an overall grade ,Date of Graduation:31-5-2017 ,Date of issue
	certificate_title	Graduation Certificate
	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

Table 0.2 : shows the global fields that are used to create the certificate template

According to the variables defined within the program, there are three main variables specific to each recipient. Which is the name, pubkey and identity.

While the selected certificate contains more fields for each recipient, such as the grade field. These fields are defined within the settings file. Consequently, the value of *additional\_global\_fields* and *additional\_per\_recipient\_fields* has been modified. The table 3.2 shows the additional fields for each recipient that will be used to create a JSON file.

Field name	Example of values
student_id_number	43404274
national_id	1085652822
degree	Bachelor
specialty	Business Administration Management
college	Administrative & Financial Sciences
gpa	3.81
grade	Excellent

Table 0.3 : The additional fields for each recipient

Then a roster of recipient data is prepared as csv file. The table 3.3 displays roster for three students that will be used to issue a batch of certificates.

name	pubkey	identity	student_id_number	national_id	degree	specialty	college	gpa	grade
ARWA ABDULLAH D AISOFYANY	ecdsa-koblitz- pubkey:mpqSQued NCrh7M8ZSCCMD W81LJjsAbH5F3	arwa@tu.gov.sa	43404274	1085652823	Bachelor	Business Administration Management	Administrative & Financial Sciences	3.81	Excellent
AHLAM AHMED S ALTALHI	ecdsa-koblitz- pubkey:mhAFL5ov 7skwaxb3wANXKn KNpTjoiaTSVr	ahlam@tu.gov.sa	43404275	1075652822	Bachelor	Business Administration Management	Administrative & Financial Sciences	3.5	Excellent
HIND MOHAMMED U ALSALMI	ecdsa-koblitz- pubkey:miBF6NjW Vv9CFibprQXJDZb VPUhxc63wMj	hind@tu.gov.sa	43404277	1095652822	Bachelor	Business Administration Management	Administrative & Financial Sciences	3.72	Excellent

Table 0.4: shows the data for students

By using cert-tools the certificate template will be designed and instantiating a certificate batch. The cert-tools setup contains 2 scripts. The first: create\_certificate\_template.py, which used to create the certificate template. The second: instantiate\_certificate\_batch.py, which adds the recipient's data. So, it creates a certificate for each recipient based on the data in csv file. Figure 3.3 and figure 3.4 show the running of the scripts.



```

MINGW64:/c/Users/LOLO/Desktop/Blockchain/cert-tools - Copy
LOLO@Elham MINGW64 ~/Desktop/Blockchain/cert-tools - Copy (master)
$ python create_v2_certificate_template.py -c conf.ini
Writing template to C:\Users\LOLO\Desktop\Blockchain\cert-tools - Copy\sample_data\certificate_templates\test.json
Created template!

LOLO@Elham MINGW64 ~/Desktop/Blockchain/cert-tools - Copy (master)
$

```

Figure 0.3 : running create\_certificate\_template script

```

MINGW64:/c/Users/LOLO/Desktop/Blockchain/cert-tools - Copy
LOLO@Elham MINGW64 ~/Desktop/Blockchain/cert-tools - Copy (master)
$ python instantiate_v2_certificate_batch.py -c conf.ini
Writing certificates to C:\Users\LOLO\Desktop\Blockchain\cert-tools - Copy\sample_data\unsigned_certificates
Instantiated batch!

LOLO@Elham MINGW64 ~/Desktop/Blockchain/cert-tools - Copy (master)
$

```

Figure 0.4 : running instantiate\_certificate\_batch script

The resulting files are stored in unsigned\_certificates folder as shown in the figure 3.5. After that, the unsigned certificates were copied to cert\_issuer.

Name	Date modified	Type	Size
1e7d263c-adc7-4065-a6f8-948489f1ef78	11/10/2018 10:31:18	JSON File	640 KB
b56c803f-fa4e-4000-941a-eeb1f112755b	11/10/2018 10:31:18	JSON File	640 KB
ee636242-6659-4ee3-a893-43754d6cdf7f	11/10/2018 10:31:18	JSON File	640 KB

Figure 0.5 : JSON files for each recipient

### 3.2 Issuing Certificates

Issuing the certificate is done by creating a transaction on the bitcoin network from the issuing institution to the recipient including the hash of the certificate.

The cert\_issuer allows the issuance of certificates in three modes: regtest, testnet and mainnet.

Regtest mode represent the local Bitcoin test environment that can generate fake coins for issuing test certificates. Testnet mode is a closer simulation to issuing certificates on the Bitcoin blockchain. However, it does not spend real Bitcoins yet. Mainnet mode which write transaction to a public blockchain as real bitcoin.

The certificate will be issued in testnet mode that uses APIs to look up and broadcast transactions by following these steps:

- 1- Install cert-issuer.
- 2- Create a Bitcoin issuing address by using bitaddress.org.

bitaddress.org" Open Source JavaScript Client-Side Bitcoin Wallet Generator"[31].



Figure 0.6 : bitaddress.org website

Figure 3.6: shows bitaddress.org website that used for getting addresses for bitcoin in testnet mode. General addresses for the testnet start with the letters M or N while they begin with the numbers 0 and 1 in the mainnet. The public key was obtained:

*Public key:* `n4eiiljvatrWFcmVs6WVzUQdNn4S5eWZFL`.

It is saved in the settings file as a value for *issuing\_address* variable. Also, we will get the private key corresponding to the public key.

*Private key:*

`cRD6dNwDTB3Ax22Z3QbdKfVghTW3qU5sQH2VmEhGAaFw8qjq1c7G`

The private key should keep confidential. It is saved as a text format and used to insert a digital signature on certificates.

- 3- Getting testnet coins by enter *Public key* in “Testnet Faucet”. Testnet Faucet is simple form of web page. The user enters the bitcoin testnet address. Thereafter, testnet faucet will send a fake bitcoin to this address. There are a large number of websites offer this service for developers for test purposes[32].

Figure 3.7 shows the faucet testnet that was used.

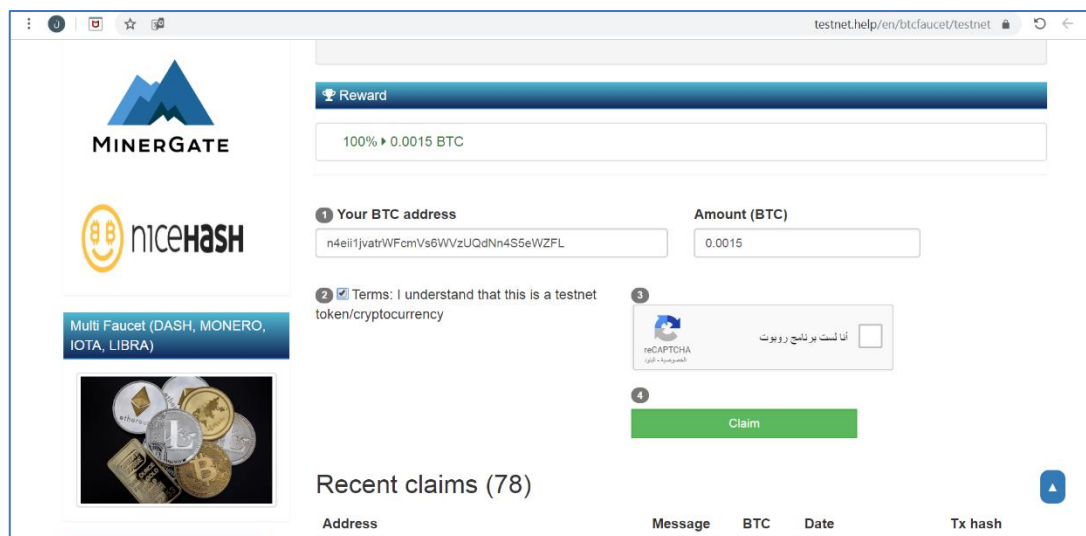


Figure 0.7 : the faucet testnet that was used

- 4- Setting file namely *conf\_template.ini* for cert-issuer is edited by determine path of folders for following variables: *unsigned\_certificates\_dir*, *blockchain\_certificates\_dir*, *work\_dir* and *usb\_name*. The type of network used is also determined as *bitcoin\_testnet*. And add unsigned certificate in *data/unsigned\_certs/* folder.
- 5- running cert-issuer. Blockchain Certificates will be saved after they are issued in *data/blockchain\_certificates* folder.
- 6- The blockchain explorer displays the transaction as shown in Figure 3.8

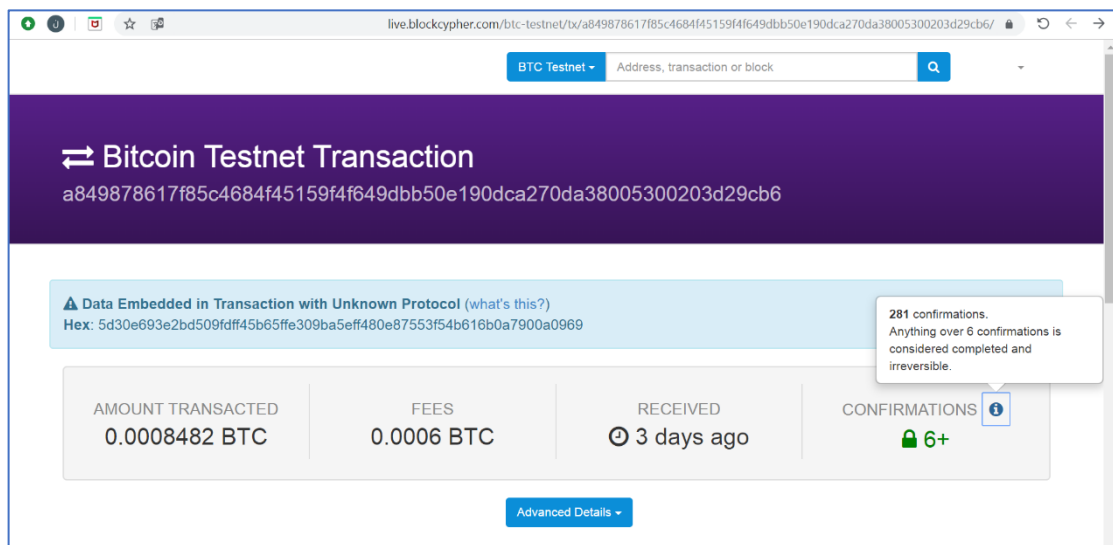


Figure 0.8 : Blockchain Explorer

Issuing each certificate separately with one transaction for each one will reduce the effectiveness of the program. Hence, batch of certificates is issued in one transaction by building a Merkle tree Which discussed previously in Chapter 2. Merkle root can be kept as the OP\_RETURN field in the Bitcoin transaction.

### 3.3 Develop Certificate viewer

This tool is used to view and validate issued certificates. It provides two website themes using different settings.

- 1- Basic configuration options which use a file system key value (simplekv\_fs) to store blockchain certificate in cert-data folder. After editing the settings file conf\_local.ini as shown in table 3.4, an application runs to show the home page of the site as in figure 3.9.

Field name	Value
recent_certids	1e7d263c-adc7-4065-a6f8-948489f1ef78, b56c803f-fa4e-4000-941a-eeb1f112755b, ee636242-6659-4ee3-a893-43754d6cdf7f
secret_key	\xe0\xfd\x7f- \x9b:0\xda?\xfd**iO\xdb d\xff\x80\xa7\xce\x8e\xbe
cert_store_type	simplekv_fs
cert_store_path	cert_data
issuer_name	TAIF UNIVERSITY
issuer_logo_path	img/logo.png
issuer_email	Taif_University@tu.org
Theme	default

Table 0.5 : content of file local.ini

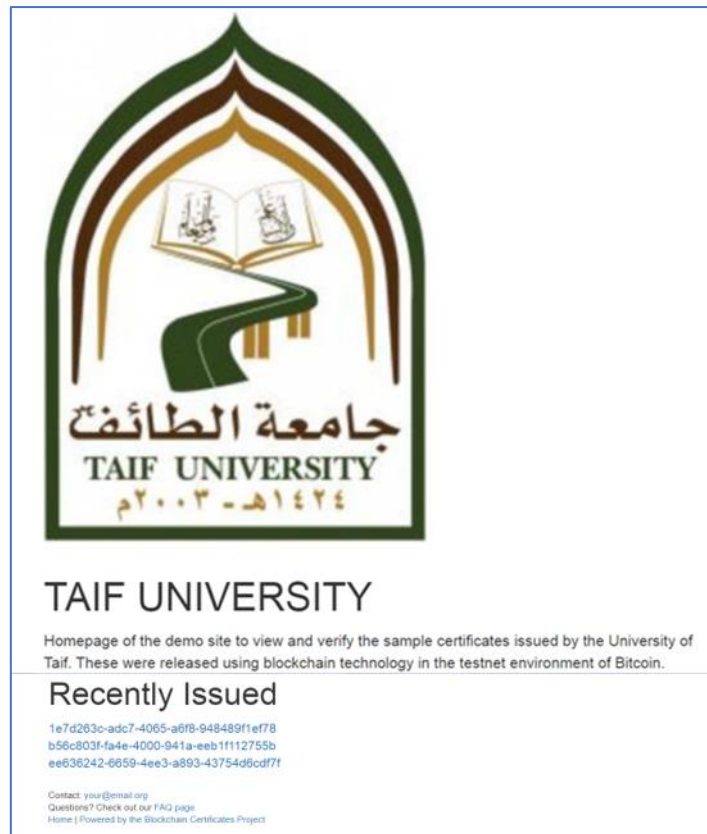


Figure 0.9 : Home page with basic configuration

Issued certificates are displayed on the home page of the site.

When one of the certificates was chosen, the website will show the next page that displays the certificate data. For purposing of adding important details for the certificate, further fields have been added in the JSON file. These fields are modified in the following files: *certificate\_formatter.py*, *model.py* and *award.html*. The certificate can be validated by clicking the *Verify* button as shown in the figure 3.10.

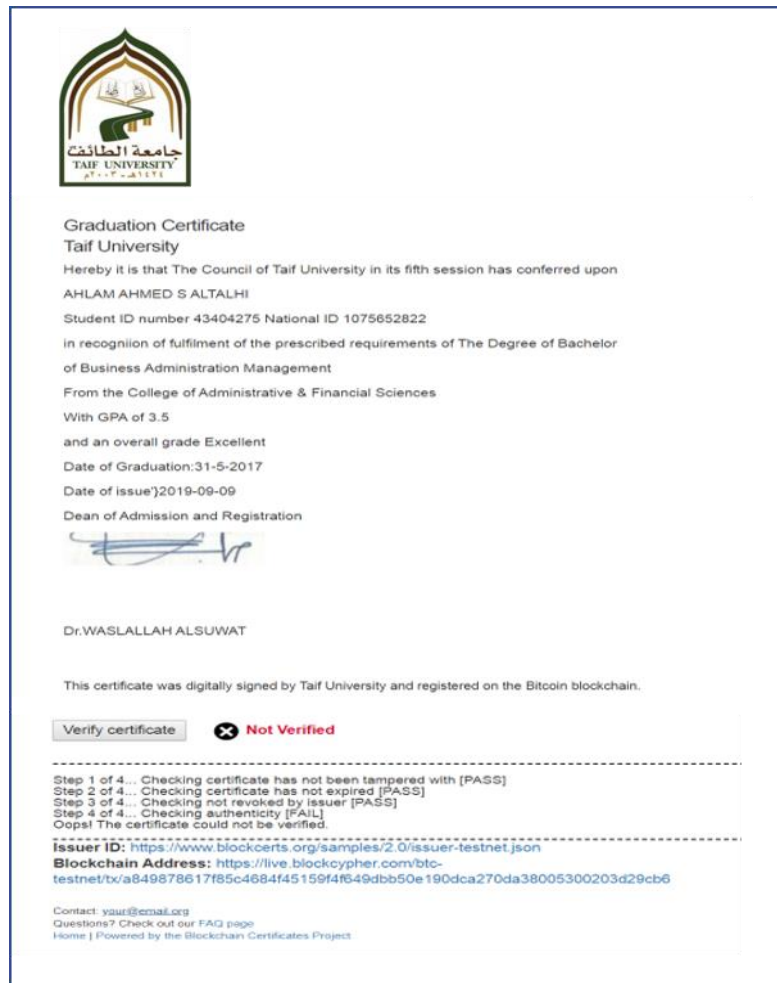


Figure 0.10 : The web page that displays the certificate data

## 2- Advanced configuration options:

The using of advanced settings options allows recipients to request certificates from educational institution. The recipient will enter the Bitcoin address or request its creation if it does not exist and enter the name and e-mail. Furthermore, the issuer can store certificate data within the Mongo database. Before run *cert\_viewer* with advanced configuration options the database server must be running, and the database created.

In file setting *conf\_template.ini* value of *cert\_store\_type* determine the type of key value store to use for the certificate. to store certificate in mongodb *simplekv\_gridfs* can be used.

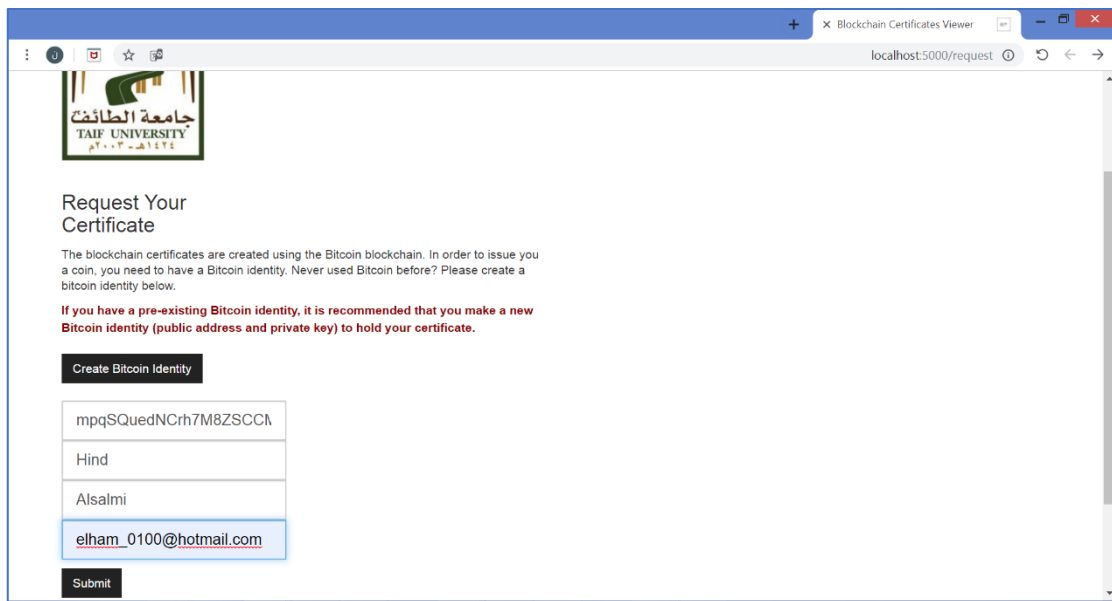
The value of *mongodb\_uri* is used to access mongo dB for storing Recipient requests. Its value is determined as follows:

```
mongodb://127.0.0.1:27017/cert
```

where "cert" is the name of database that have been created.

The cert database consists of three collections: fs.files, fs.chunks and introductions . fs.files contains metadata for files which uploaded to the database such as id,filename...etc. fs.chunks contain certificate files that have been uploaded to the database after they are issued by using `mongo-seed/load_gfs.py` script.

Introductions contains the data of the recipients who have requested their certificates. Figure 3.11 show webpage form to request certificate



The screenshot shows a web browser window titled "Blockchain Certificates Viewer" at the URL "localhost:5000/request". The page features the logo of Taif University (جامعة الطائف) and the heading "Request Your Certificate". Below the heading, there is a paragraph explaining that blockchain certificates are created using the Bitcoin blockchain and require a Bitcoin identity. A red warning message states: "If you have a pre-existing Bitcoin identity, it is recommended that you make a new Bitcoin identity (public address and private key) to hold your certificate." The form contains a "Create Bitcoin Identity" button, a text input field with the value "mpqSQuedNCrh7M8ZSCCA", a "Hind" label, an "Alsalmi" label, an email input field with the value "elham\_0100@hotmail.com", and a "Submit" button.

Figure 0.11 : webpage form to request certificate

The option to use email notifications for recipients can be activated by setting the mail value for *notifier*.

Where an account was created on the site Elastic Email for managing e-mail transactions. Hence, the API was used to send registration confirmation emails.



The *Requests* webpage allows the recipient to create Bitcoin Identity if he does not own it. The recipient clicks the *Create Bitcoin Identity* button to go to a *bitcoinkeys* webpage.

After pressing the *Generate Keys* button, the public key and the corresponding private key appear as shown in figure 3.12.

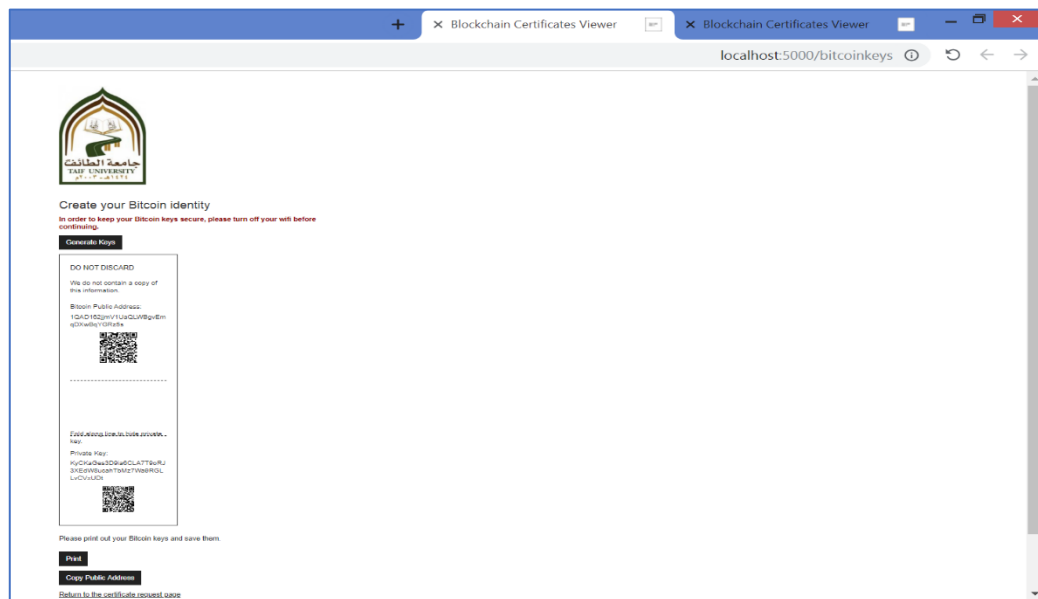


Figure 0.12 : Bitcoin keys webpage

After entering the recipient data into the form and pressing the send button. A message appears stating that the order confirmation was sent to the e-mail entered as shown in Figure 3.13.

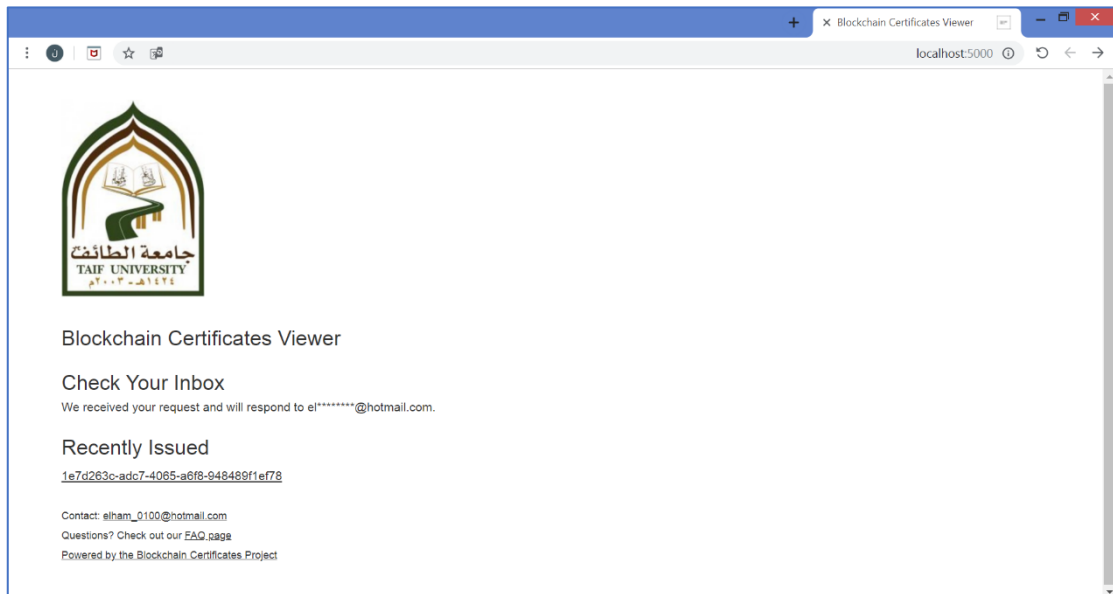


Figure 0.13 : message request confirmation

## CHAPTER 4: Verification and Evaluation

### 4.1 Verification Process:

The python [cert-verifier](#) library is used to validate the blockchain certificates. In this section, we will discuss the details of the verification process.

The certificate contains the content to be verified and the additional entries needed for the verification process.[33]

A Blockchain Certificate must have

a `certificate.signature.anchors` field, which must contain at least one anchor to a blockchain transaction.

anchors as shown in figure 4.1 filed contains three fields:

- 1- `sourceId`: This field specifies the transaction number  
"sourceId":  
"a849878617f85c4684f45159f4f649dbb50e190dca270da38005300203d29cb6"
- 2- `type`: the value of Field "BTCOPReturn" indicates that field `OP_RETURN` is used in the certificate the integrity of the certificate.
- 3- `chain`: shows that the transaction was performed on the Bitcoin testnet

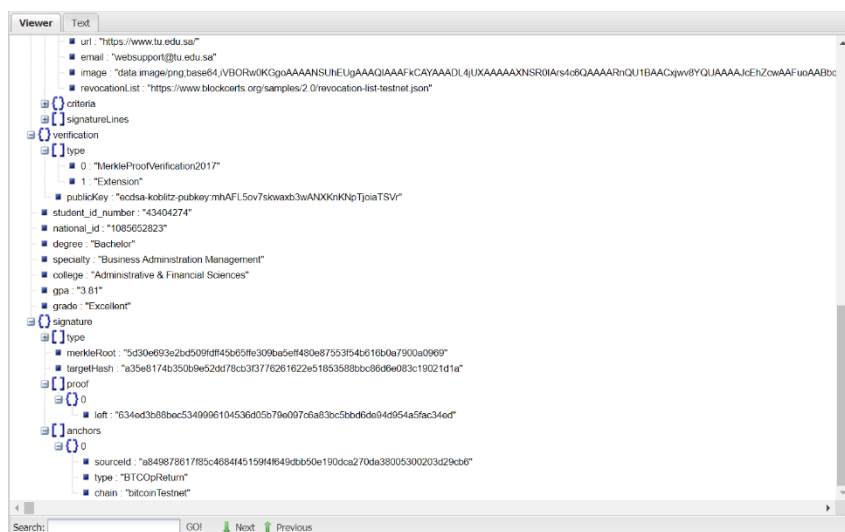


Figure 0.1 : anchors filed

Field `badge.issuer.id` is used to identify the issuer of the certificate .It shows where to find information about the issuer. currently using HTTP URL for issuer as identity information is required to verify the issuer's claim to have public keys.

### Check certificate integrity:

The checking of certificate integrity ensures that the certificate has not been manipulated. This consists of 3 steps

- 1) Validate the Merkle proof in the certificate: Blockcerts uses the Verifiable Claims MerkleProof2017 signature format, which is based on Chainpoint 2.0. It is verified that hash of specific data is related to the blockchain. It proves that the data is existing at the previously established time. It connects hash data to the blockchain and returns the timestamp proof.
- 2) The certificate hash value is calculated and compared to the hash value in the signature field. The project uses JSON-LD canonicalization to ensure a stable arrangement of the contents of the Json file. Depending on the JSON-LD signature configuration, it removes the signature portion of the certificate, then the hash value is calculated using SHA-256.The resulting value must be the same as the value in the *signature.targetHash* field
- 3) Compare the value of Merkle Root in the certificate with the value in the blockchain transaction. Figure 4.2 shows signature fields.

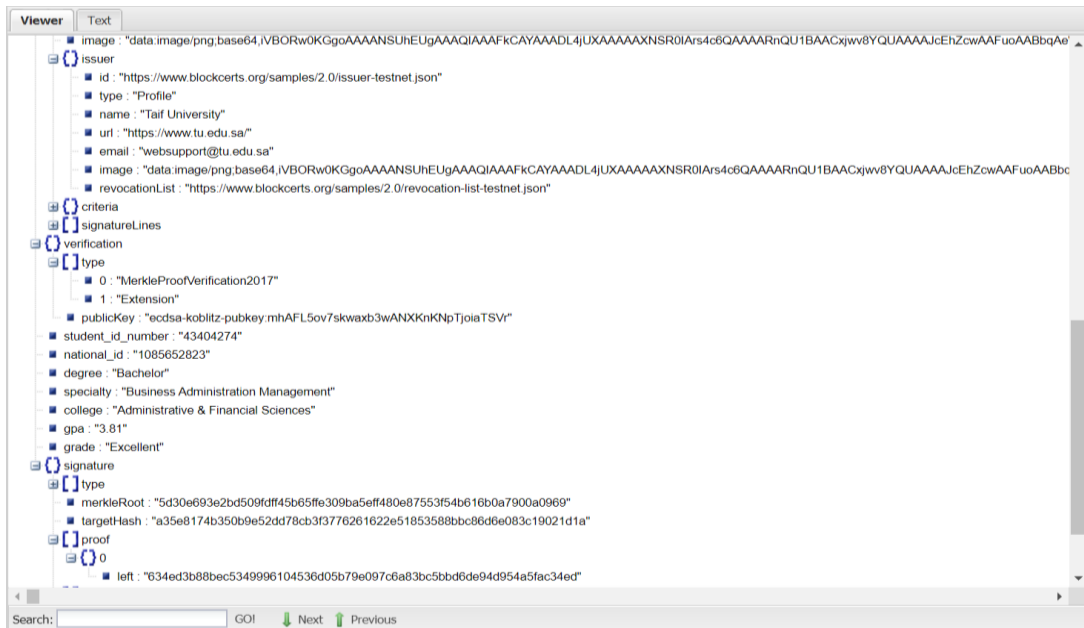


Figure 0.2 : signature fields

### Check certificate authenticity

In this step, it is verified that the Issuer issued the certificate using the time stamp and the address of the Issuer in the transaction details. The testnet mode does not provide the ability to verify the authenticity of the certificate.

### Check not revoked by an issuer:

Source revocation data contains a list of revoked certificates IDs and revocation reasons. Cancellation of the certificate cannot be verified in testnet mode.

### Check certificate has not expired:

Some types of certificates may expire after a certain period. In this case, the end date is entered into the expire field and compared to the current date during the verification process. For the sample certificates used, there is no expiration date.

## 4.2 Evaluation of security requirements

### 1) integrity of a certificate:

There are many security aspects of blockchain-based systems. For security requirements assessment, we will focus on testing the integrity verification of a certificate. This will be accomplished by a trial of deletion and changing some of the previously processed certificate values. So, the system should identify this manipulation as a part of certificate validation.

The main libraries of the project include a sample of differently designed certificates. Due to these differences, the required variables for selected certificates were defined. As a result, the program does not display any certificates that do not contain additional fields. Also, the program does not display any certificate that does not contain a digital signature

The issued certificates cannot be updated but can be revoked in case of error. The data in the certificate can never be changed. The verification process of certificate contents cannot manipulate. The certificate contains two different types of data, text and images. Certificate data is represented in the JSON file format. JSON file viewer was used to see the data more clearly. As noted, all the contents of this file are textual, including pictures of the university's logo and signature.

The data of the issued certificates has been changed to test the integrity verification function. The changes made included adding, deleting, and modifying. The verification tool showed that the certificate was not valid when performing any of the previous operations.

The table 4.1 summarizes the certificate number, an attempt to change the data that was performed on it, and the result that the validator showed

id	Modification type	filed	Value before Modification	Value After Modification	Verification result
1e7d263c-adc7-4065-a6f8-948489f1ef78	Change value	gpa	3.5	3.9	Not Verified
b56c803f-fa4e-4000-941a-eeb1f112755b	Delete value	collage	Administrative & Financial Sciences	-	Not Verified
ee636242-6659-4ee3-a893-43754d6cdf7f	Adding value	grade	Excellent	Excellent With first honors	Not Verified

Table 0.1 : Result of validation process after modification

For images, they are converted to text using the Base 64. It is a widely used system on the World Wide Web. Base64 is a " set of binaries to text encoding charts representing binary data in ASCII string format. It is designed to reliably transmit data across channels that support text content. One of its most important uses is to include image files within binary text assets" [34]. Use of this image encoding system provides constant hashing of the JSON file. The table 4.2 displays one of the images in the certificate and the corresponding value when using the Base64


Image	
Image after encoding to base64	"data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAgwAAABwCAYAAAEF/hgKAAAAAXNSR0IArs4c6QAAAARnQU1BAACxjwv8YQUAAAJcEhZcwAAAFxEAABcRAcom8z8AAP+1SURBVHhezP0F11JkiWMzqp/+NZ6M9PTUF2dVckMyhQzKxQK KUDBzMwMUjAzM+NlvkH77e0nrlKpyuqunq/nexO ZpnPuQT/uZtvM3M3N/9vZ+THOzk/gDfiRkZ0Fp8eN 8OkJTgGEzoMInYVwdnaMk2AAZ+EQTk7Cp16PHz lZhQgFQwgfexDyOxAOOuF1HcBh28EJj52d+nES8i Mc8OI46MNx2I/TMJ9xEoLHeYQQj5/wuM6fnvC6k Bte5wGPO+G27/E4nxvkPbw+HPLB73fB53Ni6/AQL xPSMb+4hvOzc4TDHpyfnp06/DvwnATxx49+5LvPs H+4DYfLeo/f5QAfBAQ...

Table 0.2 : Image and value of encoding to Base64

## 2) Storing certificate data :

The content of the certificate is not stored on the blockchain network. What is stored only is the hash value that allows third parties to verify the validity and integrity of the certificate. Accordingly, the issuing authority must follow clear policies regarding storing certificates to avoid losing the certificate. It is not entirely reliable to host the issuer to the certificate since the issuing site may stop working temporarily as a result of a technical malfunction or become permanently out of service. If the issuer does not want to host the certificate permanently, recipients must be notified to keep the certificate by downloading it or importing it into the wallet. The certificate's JSON file can also be sent as an attachment in an email. Here we stress the necessity of correct recipient addresses. A student's university email can be used to send a copy of the certificate

## 3) Get recipient data:

In Chapter three, the researcher discussed how the web-based certificate request form provides the ability to request a Bitcoin address. It also allows the recipient to enter other data required to issue the certificate, such as name and email address, and send it to the issuing authority. This data is stored in the database for use when issuing certificates. The issuer must verify the validity of recipient data and absence of duplicate requests to ensure the authenticity of the issued certificates

## 4) Verify the identity of the issuer and the recipients:

This project does not allow the registration process and assigning public keys to organizations or individuals. Accordingly, any authority can



issue certificates, and recipients can provide any address to submit request to get digital certificate

From the architectural perspective of Bitcoin, separation of identity and addresses is desirable. But for this project, it is necessary for issuers to verify identity. One possible way to do this is to use an organized profile like Blockstack profiles.

#### 5) Keys management:

The keys management issue is one of the most important security issues still to be discussed. Whereas the loss or theft of keys is considered the most prominent threat to any cipher system.[35]

The system relies on storing keys in the local storage of the device. The keys can be accessed by Bitcoin from the Bitcoin configuration file. This method is fast and easy to access keys for any Bitcoin transaction, but this Some type of system is not safe from device corruption, malware, hackers

The certificate file's settings file includes offline key activation mode to avoid the potential for online piracy. The program also indicates the necessity of storing the issuer's private keys in secure portable media without an Internet connection such as USB. However, the risk of losing or damaging storage media remains. Losing the private key of the issuer may result in the issuance of fake certificates.

For recipients, the certificate request form provides the ability to generate the pair of keys as discussed in the third chapter. The keys are displayed as text and a QR-code on the web page. The recipient is alerted about the need to keep keys safely because it is difficult to retrieve the key. Therefore, the recipient may be losing the ability to verify ownership of the certificate without those keys.

### **4.3 Evaluation of privacy requirement**

There are several factors that determine how well a project meets privacy requirements. By design, the Bitcoin network provides privacy to the user. But must be a balance between security and privacy and the availability of data necessary for the verification process.

The selected certificate contains sensitive data such as civil registration number and grade point average. It is important to maintain this data and not to show it to the public. Private information is not available on the blockchain. What is stored on the blockchain network is the hash value of the certificate. As we indicated in Chapter Two, it is practically impossible to obtain the original data from the hash value. Thus, only the intended parties can verify the certificate by calculating the hash value of the certificate and comparing it to the value stored on the blockchain.

The options for publishing blockchain certificates are important to study the project's compliance with privacy requirements.

In Chapter Three, a webpage was used to display the issued certificates. When clicking on the certificate number, another page displays the content of the certificate. This method was used to display the certificates attached with the project as examples, but the certificates did not contain sensitive information. Regarding the present sample of chosen certificates, this method is considered inappropriate since these certificates contain personal information that should be protected from public disclosure.

## CHAPTER 5: Conclusion

### 5.1 Discussion Results:

According to project evaluation and discussion in the chapter four, the program demonstrated the ability to preserve the contents of the certificate from any attempt to change the content.

Regarding the privacy requirements, the sample of selected certificates contain sensitive data. However, the certificates are displayed as links on the main page of the hosting provider. Hence, it does not meet the privacy requirements.

Further suggestions for project development may include several ideas. Such as searching for possible ways to confirm the identity of both issuers and recipients through integrate the identity with the projec. in addition to Find effective solutions to a problem place of certificate storage and recipient request processing to make the system suitable for application.

The success of systems based on blockchain technology depends on the interaction of several bodies, so the availability of a unified infrastructure for the system that meets the requirements of these bodies is important manner. In addition, it is one of the solutions to address the problem of interoperability. Therefore, the adoption of technical projects by governments is one of the important factors for the effective participation of educational institutions, employment agencies and individuals in this system.

### 5.2 Future work:

Testnet mode provides developers with complete verification of certificate integrity and is one of the steps in the verification process.

According to the developers of the project, the testnet mode does not allow developers to verify the authenticity and revocation of the certificates

referred to in Chapter 4[36]. Therefore, the future work of this research will focus on the following aspects:

- 1) Application of the program to real data and publishing certificates on the main network
- 2) Discuss ways to verify the originality of the issuing body
- 3) Discuss ways to revoke certificates



## References

- [1] Wikipedia. (2019, 08 July). *Blockchain*. Available: <https://en.wikipedia.org/wiki/Blockchain>
- [2] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learning Environments*, vol. 5, no. 1, p. 1, 2018.
- [3] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," *PloS one*, vol. 11, no. 10, p. e0163477, 2016.
- [4] Media Lab Learning Initiative and Learning Machine. (2019, 13 July). *Digital Certificates Project*. Available: <https://certificates.media.mit.edu/>
- [5] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *European Conference on Technology Enhanced Learning*, 2016, pp. 490-496: Springer.
- [6] A. Grech and A. F. Camilleri, "Blockchain in education," ed: Luxembourg: Publications Office of the European Union, 2017.
- [7] G. Zyskind and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, 2015, pp. 180-184: IEEE.
- [8] I. B. Bandara, F. Ioras, and M. P. Arraiza, "The emerging trend of blockchain for validating degree apprenticeship certification in cybersecurity education," 2018.
- [9] K. Kuvshinov, I. Nikiforov, J. Mostovoy, D. Mukhutdinov, K. Andreev, and V. Podtelkin, "Disciplina: Blockchain for Education," ed, 2018.
- [10] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE access*, vol. 6, pp. 5112-5127, 2018.
- [11] J. Cheng, N. Lee, C. Chi, and Y. Chen, "Blockchain and smart contract for digital certificate," in *2018 IEEE International Conference on Applied System Invention (ICASI)*, 2018, pp. 1046-1051.
- [12] R. Li, "Better Security Over Blockcerts," MSc, Computer Science, The University of Birmingham, 2017.

- [13] P. Ocheja, B. Flanagan, H. Ueda, and H. Ogata, "Managing lifelong learning records through blockchain," *Research & Practice in Technology Enhanced Learning*, Article vol. 14, no. 1, pp. 1-1, 2019.
- [14] M. m. c. a. k. Choi, S. R. r. c. a. k. Kiran, S.-C. s. g. c. Oh, and O.-Y. o. k. a. k. Kwon, "Blockchain-Based Badge Award with Existence Proof," *Applied Sciences (2076-3417)*, Article vol. 9, no. 12, pp. 2473-2473, 06/15/ 2019.
- [15] Open Source University. (2019, 31 July). *Open Source University*. Available: <https://os.university/>
- [16] B. Singhal, G. Dhameja, and P. S. Panda, *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*. Springer, 2018.
- [17] E. Elrom, "The Blockchain Developer."
- [18] C. Paar and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.
- [19] N. Storublevtcev, "Cryptography in Blockchain," in *Computational Science and Its Applications – ICCSA 2019*, Cham, 2019, pp. 495-508: Springer International Publishing.
- [20] D. Drescher, *Blockchain basics*. Springer, 2017.
- [21] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352-375, 2018.
- [22] z. i. a. c. Rui Zhang, x. i. a. c. Rui Xue, and l. l. c. g. e. Ling Liu, "Security and Privacy on Blockchain," *ACM Computing Surveys*, Article vol. 52, no. 3, pp. 1-34, 06// 2019.
- [23] W. Stallings, *Cryptography and Network Security, 4/E*. Pearson Education India, 2006.
- [24] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: techniques, applications, and challenges," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, 2018, pp. 1-11: IEEE.
- [25] Z. Liu *et al.*, "A survey on blockchain: a game theoretical perspective," *IEEE Access*, vol. 7, pp. 47615-47643, 2019.
- [26] Packt. (2020, 01 MARCH). *Exploring Blockchain and BaaS*. Available: <https://subscription.packtpub.com/book/data/9781789804164/1/ch01lv1sec06/layered-structure-of-the-blockchain-architecture>

- [27] Blockchainhub Berlin. (2020, 01 March). *Decentralized Applications – dApps*. Available: <http://blockchainhub.net/decentralized-applications-dapps/>
- [28] Malcoded.com. (2020, 04 March). *Storing Data on the Blockchain: The Developers Guide*. Available: <https://malcoded.com/posts/storing-data-blockchain>
- [29] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: current status, classification and open issues," *Telematics and Informatics*, 2018.
- [30] B. Smith, *Beginning JSON*. [Berkeley, CA]: Apress, 2015.
- [31] (2019, 28 September). *Bitaddress.org*. Available: <https://www.bitaddress.org/bitaddress.org-v3.3.0-SHA256-dec17c07685e1870960903d8f58090475b25af946fe95a734f88408cef4aa194.html?testnet=true>
- [32] brave. (2019). *Bitcoin Faucet Testnet*. Available: <https://testnet.help/en/btcfaucet/testnet>
- [33] BLOCKCERT. (2019, 19 DEC 2019). *blockchain-certificates/cert-verifier-js*. Available: <https://github.com/blockchain-certificates/cert-verifier-js/blob/master/docs/verification-process.md>
- [34] wikipedia. (2019). *Base64*. Available: <https://en.wikipedia.org/wiki/Base64>
- [35] O. Pal, B. Alam, V. Thakur, and S. Singh, "Key management for blockchain technology," *ICT Express*, 2019.
- [36] kim. (2019, 19 DEC 2019). *Regtest certificate verified on blockcerts page*. Available: <https://community.blockcerts.org/t/regtest-certificate-verified-on-blockcerts-page/1050/2>