Introduction

1.1Motivation

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.