Authentication System of Online Student Profiles with Blockchain Algorithm

Sermet Eser Özvataf

Submitted to the
Institute of Graduate Studies and Research
in partial fulfillment of the requirement for the degree of

Master of Science
in
Information and Communication Technologies in Education

Eastern Mediterranean University
February, 2019
Gazimagusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Assoc. Prof. Dr. Ali Hakan Ulusoy
Acting Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science in Information and Communication Technologies in Education.

Assoc. Prof. Dr. Ersun İşçioğlu
Acting Chair, Department of Computer Education and Instructional Technologies

We certify that we have read this thesis and that in our opinion; it is fully adequate in scope and quality as a thesis for the degree of Master of Science in Information and Communication Technologies in Education.

Assoc. Prof. Dr. Ersun İşçioğlu
Supervisor

Examining Committee

1. Assoc. Prof. Dr. Ersun İşçioğlu

2. Asst. Prof. Dr. Fahme Dabaj

3. Asst. Prof. Dr. Fatma Tansu Hocanın

ABSTRACT

Nowadays, use of internet by more people made the demand towards online education increase. Together with the integration of education and technology, these trainings have become available as a new channel on digital platforms. Therefore, educational institutions, especially universities and private enterprises have started to offer courses they provide in physical settings in online platforms as well. Just as in the courses given in the physical settings, when the determined learning outcomes are achieved, this success is documented through certificates or diplomas. Although, the concepts such as educational content and student information in educational institutions' own information systems are not digitally portable and shareable, it still needs a lot of work flow based on manpower and physical documentation which carries qualities that lack behind the online technologies, unreliable and also not without integration problems. In the scope of this work, it is aimed to provide a system where the data of the educational background of individuals can be stored and verified using blockchain algorithms. Blockchain is a distributed recording system that can be shared by many parties, facilitating the recording of new processes while making it easier to monitor over the network of an unbreakable data set. Along with the fact that data security, verifiability and durability can be ensured in electronic form by using only blockchain, it also enables learning records to be stored and shared without a central authority. Another advantage of verifiability is to prevent imitation of the identity and documents of educational institutions and to protect the dignity of both academic and non-academic institutions. In addition to the basic facilities provided by the Blockchain system, the new possibilities and uses that come up with the combination of learning needs and technology are evaluated. It is an example of the fact that students are not limited to the educational opportunities of an educational

institution but can also provide the educational resources of the fields they want to specialize from different educational institutions. The educational plans that can be obtained through digitalized data are considered as new advantages that can be offered to institutions and education designers. This study goes through an exemplary application design to address the assessments identified.

Keywords: Blockchain, Certification, Diploma, Transcript, E-Learning, Educational Technologies, Information Systems, Verification

ÖZ

Günümüzde, internetin daha çok insan tarafından kullanılır hale gelmesi, online eğitimlere olan talebi arttırmıştır. Eğitim ve teknolojinin entegrasyonu ile birlikte, talep edilen bu eğitimler yeni bir kanal olarak dijital platformlar üzerinden de arz edilebilir hale gelmiştir. Bu nedenle; üniversiteler ve özel girişimler başta olmak üzere, eğitim kurumları fiziksel ortamlarda verdikleri dersleri online olarak da sunmaya başlamışlardır. Fiziksel ortamlarda verilen derslerde olduğu gibi, belirlenen eğitim hedeflerine ulaşıldığında bu başarı durumu sertifikalar veya diplomalar aracılığıyla belgelendirilmektedir. Ancak eğitim kurumlarının kendi bilgi sistemlerinde yer alan eğitim içeriği ve öğrenci bilgisi gibi kavramlar dijital anlamda taşınabilir ve paylaşılabilir niteliklerde olmadığı için online teknolojilerin gerisinde kalmış, güvenilebilirlik ve entegrasyon sorunları nedeniyle halen fiziksel evrak ve insan gücüne bağlı birçok iş akışına gereksinim duymaktadır. Bu çalışma kapsamında; blockchain algoritmaları kullanılarak bireylerin eğitim geçmişlerine ait verilerin saklanabildiği ve doğrulanabildiği bir sistem sunmak amaçlanmaktadır. Blockchain, bütünlüğü bozulamaz bir veri dizisi üzerinde yeni işlemlerin kaydedilmesini ve bunların ağ üzerinden izlenme sürecini kolaylaştıran, birçok parti tarafından paylaşılabilir, dağıtık bir kayıt sistemidir. Yalnızca blockchainden yararlanılarak, elektronik ortamda veri güvenliği, doğrulanabilirliği ve kalıcılığı sağlanılabilmekle birlikte; bir merkezi otorite olmaksızın öğrenim kayıtları saklanılabilir ve paylaşılabilir. Doğrulanabilirliğin getirdiği bir diğer avantaj eğitim kurumlarına ait kimlik ve evrakların taklit edilmesi önlemek ve hem akademi hem de akademi-dışındaki dünya için kurumların itibarlarının korunmasını sağlamaktır. Blockchain sisteminin sağladığı temel imkanlara ek olarak, öğrenim ihtiyaçları ve teknolojinin birleşimiyle açığa çıkan yeni olanak ve kullanımlar da değerlendirilmektedir.

Öğrencilerin bir eğitim kurumunun eğitimsel olanakları ile sınırlı kalmayıp uzmanlaşmak istedikleri alanlara ait eğitim kaynağını farklı eğitim kurumlarından temin etmesi buna bir örnektir. Yine dijitalleşmiş veri sayesinde elde edilebilecek eğitim planlamaları bir eğitim teknolojisi olarak kurum ve eğitim tasarımcılarına sunulabilecek yeni faydalar olarak düşünülmektedir. Bu çalışma saptanan değerlendirmeleri ele almak için örnek bir uygulama tasarımı üzerinden gitmektedir.

Anahtar Kelimeler: Blockchain, Sertifikasyon, Diploma, Transkript, E-Öğrenme, Eğitim Teknolojileri, Bilgi Sistemleri, Doğrulama

ACKNOWLEDGEMENT

Before starting with the study, I would like to thank people who were with me through this process.

At first, I would like to express my deepest gratitude to my supervisor Assoc. Prof. Dr. Ersun İşçioğlu for his guidance and constant encouragement throughout the writing of this thesis. His positive outlook, confidence in me and valuable moral support have always inspired me to greater efforts.

I owe a huge thank you to my wife Şeyma Özvataf who have experienced all of the ups and downs of my research with me. She has patiently and lovingly supported me throughout my life.

Further, I would also like to thank my friends Arda Kılıçdağı and Onur Babacan for their inputs and support during my research.

To conclude, I would like to thank all the educators that endeavor raising generations for the bright future.

TABLE OF CONTENTS

ABSTRACT iii

ÖZ v

ACKNOWLEDGEMENT vii

LIST OF TABLES xii

LIST OF FIGURES xiii

LIST OF ABBREVIATIONS xiv

1 INTRODUCTION 1

1.1 Problem Statement 5

1.2 Aim of the Study 7

1.2.1 Research Questions 7

1.3 Significance of the Study 8

1.4 Definition of Terms 8

2 LITERATURE REVIEW 10

2.1 Online Education 10

2.1.1 History of Online Education 11

2.1.2 Definition of Online Education 14

2.2 Blockchain Technology 15

2.2.1 Ledgers 16

2.2.2 Blockchains as Public Ledger 17

2.2.3 Blockchain in Aspect of Social Values 18

2.2.3.1 Self-Sovereignty and Identity 19

2.2.3.2 Trust 19

2.2.3.3 Immutability 20

2.2.3.4 Disintermediation 22

2.2.4 Record Types in Blockchains 22
2.2.4.1 Transactions 22
2.2.4.2 Smart Contracts 23
2.2.5 High-Level Architecture Overview 23
2.3 Certification 25
2.3.1 Components of a Certification 26
2.3.2 Processes of Certification 26
2.3.3 Standardized Processes for Issueing and Certification 27
2.3.3.1 Mechanisms for Regulation and Security 28
2.3.3.1.1 Security Features 28
2.3.3.1.2 Accessibility 28
2.3.4 Use of Certification in Education 29
2.3.4.1 Use of Certificates for Learners 29
2.3.4.2 Use of Certificates for Accreditation 30
2.3.5 Use of Intellectual Property Tracking Certificatesik 31
2.3.6 Use of Financial Certificates 32
2.3.7 Limitations of Certificates 32
2.3.7.1 Limitations of Paper Certificates 32
2.3.7.2 Limitations of Non-Blockchain Certificates 33
2.4 Digital Certificates with Blockchain 34
2.4.1 Ideal Properties for the Recipient 35
2.4.2 Ideal Properties for the Issuer 35
2.4.3 Other Properties 36
2.4.4 Certify Identity with a Blockchain 36
2.4.5 Use a Certified, Autocratic Identity 37
2.5 Issuing the Certification with Digital Signatures 37

2.5.1 Contents of a Digital Signature 37
2.5.2 Signing Documents with Digital Signature 38
2.5.3 Validating Digital Signatures 38
2.6 Blockchain-Secured Digital Certificates 39
2.6.1 Advantages 39
2.6.2 Architecture 40
2.6.3 Certification of Self-Sovereignty 42
2.7 Use Cases for Blockchain Technology in Education 43
2.7.1 Open University (UK) 43
2.7.2 University of Nicosia 44
2.7.3 Bitcoin for Payment 45
2.8 Related Research 46
2.8.1 Blockcerts 46
2.8.2 Cardano 47
3 IMPLEMENTATION 48
3.1 User Stories and Features 48
3.1.1 Business Requirements 48
3.1.2 Functional Requirements 48
3.2 Design of the PoC 50
3.2.1 Design Overview 50
3.2.2 Design and Development Tools 52
3.2.3 System of Smart Contracts 52
3.2.4 Data and Variables on the Blockchain 53
3.3 Running Steps of the PoC 54
4 EVALUATION 55
4.1 Description of Evaluation Criteria 55

4.2 Fulfilment of Evaluation Criteria 55
4.2.1 Potential Security and Privacy Exploits 56
4.3 Outcome 57
5 CONCLUSION 59
5.1 Generalisation and Extension Into Other Domains 59
5.2 Future Work 60
REFERENCES 61
APPENDICES 68

LIST OF TABLES

Table 1. User stories defining functional requirements and guiding development of authentication system PoC 49

Table 2. Evaluation of user story acceptance based on the authentication system PoC 56

LIST OF FIGURES

Figure 1. Historical background of the internet (sabri.org) 12

Figure 2. A sample ledger content (Newman, 2017) 16

Figure 3. A sample trust & recognition flow (Camilleri, 2017)..... 31

Figure 4. Digitally signed documents in a blockchain (Schmidt, 2017)..... 41

Figure 5. Issuing a blockchain-secured certificate (Schmidt, 2017)..... 42

Figure 6. A blockchain-secured self-sovereignty architecture (Grech & Alex, 2017) 43

Figure 7. University of Nicosia index of certificates 45

Figure 8. A sample process for verification of certificates in blockchain (Blockcerts, 2016) 47

Figure 9. Overview of different actors and their interactions with the blockchain and system of smart contracts which exist on the blockchain 49

Figure 10. High-level system overview of the authentication system PoC. Visualisation technique is based on (Brown, 2016)..... 51

LIST OF ABBREVIATIONS

CA	Certificate authority
ISO	International Standardisation Organisation
KMI	Open University Knowledge Media Institute, UK
P2P	Peer to Peer
PKI	Public Key Infrastructure

Chapter 1

INTRODUCTION

The impact of the internet has affected our lives and most of our exercises from day to day. In particular, the speed and diversity of products brought with them for communication and data exchange has centralised society for more data today. Almost every action in our lives every day is affected by varying degrees. These developments are exceptionally rapid in areas of change, communication, education and science. The web has been widely admired, expanded and accelerated for demonstration purposes, and emerged in a modern interchange style. The improvement of the web has also led to rapid changes in the management region. Workflows and bureaucratic forms in government life are organized gradually. No doubt, the instruction contributes to this situation. Progress is a precursor to the expansion of teaching strategies. As a common result of this situation, the directive is increasingly becoming an innovative region. The use of innovation in education, paper pen blackboard quartet to the computer and web quickly passes. This resulted in the presentation of e-learning as a result of education (Allan and Sailor, 2010; Fritz, 2011).

Using internet and computers, alternative solutions to time and space problems are the main causes of problems and limitations in education. Learning models have been proposed and developed to make students more comfortable, free and efficient. Nowadays, numerous learning-based and technology-based training model a training model that covers, is seen by many educators as an alternative educational model for the future (Tallent-Runnels, et al., 2006).

The distance learning model, which aims to eliminate high cost, time and space problems in the traditional educational environment, is an ideal learning option especially for working people. This model, which was initially used for all common educational applications, is widely used in formal education (US General Accounting Office, 2002).

Distance education, distance education and remote learning is a comprehensive concept that covers all aspects of. Distance education is the process carried out by the instructor for students and distance learning is the process carried out by the student. Therefore, it is a term that combines distant education, teaching and learning objects (using data to develop online courses).

The concept of e-learning is an intensive remote learning model for computers and the internet. In this model, students can be provided with educational services, regardless of time and space, by using the opportunities offered by the computer and the internet. Web-based training (WTE) is a term used for "web" or "World Wide Web" Services, the most widely used interface for internet education. This course model is also called "online courses" because it is always flexible over the internet (Watson and Watson, 2007).

The main purpose of this training model is to provide a wide population with the education they need and where they want. This flexibility, offered to online interns, facilitates training by increasing the efficiency of education by repeating the issues of deficiency, learning speed and testing capabilities. This can be an important contribution to formal education (WCET, 2009).

The use of technology in education is rapidly increasing. Developing technologies are inevitably being used more and more to address the growing problems of societies and to meet their needs. In front of these technologies, there are technologies such as computer and communication internet, which are called

Information Technology. Computers' computing, storage and multimedia capabilities are increasing day by day. Internet and communication infrastructure technologies are evolving at an incredible rate, and, of course, all these developments bring along many opportunities that have not existed before (Zhao et al., 2005).

Internet is moving towards network-based and platform-based social and economic models. Because assets can be shared, not only new events are offered, but new business models and self-organizing social organization opportunities are also offered. Blockchain, a developing technology, allows many financial and non-financial activities to be carried out without the need of a third-party. A blockchain consists of a set of information blocks that are securely connected to each other. Subscribers define new blocks when creating new information or changing existing information about a business (for example, transaction records, status changes, new market prices, or new owners saved). After the first block, the newly created existing blocks are securely combined with the previous trusted block. Thus, the reliability of blocks is provided as a reliable test proof. The main motivation for these processes is the creation of a reliable architect (Mamoria, 2017).

Blockchain is considered the most important technological innovation in Bitcoin. Because all processes on the network require trust and are a mechanism of trust along with the blockchain. Users rely on a public system that consists of many non-centralized, globally stored nodes managed by miners. A "blockchain" that can be translated as a "linked record array" or "linked transaction blocks" or "transactional blockchain" means a record of transaction records on the internet and on private computer networks that can be stored as contiguous process. Blocks cannot change the web (World wide web) that can then be tested, programmed, and run on the internet or on private computer networks. Participants do not need to create or maintain trust

in the bank or a third-party. Blockchain is an important innovation at barrier level as a new architecture for central and unreliable operations.

Blockchain technology is a growing interest for today. Blockchain, a relatively new innovation in information technology, is a global, inter-sectoral and disruptive innovation expected to accelerate global economic growth in the coming years (Byrne, 2017). Blockchain is the underlying technology of first cryptocurrency named bitcoin. It has the potential to convert the existing internet from The Information Exchange Internet to the value exchange internet. Blockchain technology aims to revolutionize trade, industry and education and to accelerate the development of an information-based economy. Due to their variability, validatibility and stability in all updates running on the blockchain, this innovative solution offers many uses (Marvin, 2017).

Blockchain technology did not attract much attention when it was released. However, since bitcoin has always been safe and stable over the years, the company has implemented not only the enormous potential of the fundamental technology of this invention. Blockchain technology has gain popularity among institutions, companies and researchers. Today, blockchain technology is used in a variety of fields, such as finance cryptography, Bitcoin and Ethereum.

Bitcoin is the first peer-to-peer payment system based on electronic money. A basic feature of blockchain technology is how many nodes in a distributed blockchain network come together and the bitcoin blockchain network uses a mixed-based work proof distribution algorithm. Ethereum is a distributed platform with public, block-based, open source technology and smart contract functionality that uses consensus algorithm to prove stock evidence. Zcash is a decentralized electronic money such as Bitcoin. However, it offers enhanced data protection and more selective transaction observation by using a consensus algorithm to prove zero information. Zcash payments are posted in a public blockchain. However, the sender remains exclusive to

the recipient and the amount of a transaction. In addition, some organizations and companies are trying to make development on blockchain platforms. As an example, Ubiquity is a property management company and uses the blockchain platform for providing and tracking records securely (McKinsey, 2016).

Swan (2015) said the development of blockchain applications has been divided into versions. Blockchain 1.0 is the use of cryptocurrencies as a peer-to-peer cash payment system. Blockchain 2.0 is a comprehensive blockchain application for simple cash transactions, including stocks, bonds, loans, smart Realtors and smart persons. Blockchain 3.0 develops blockchain applications that go beyond currencies, finance and Markets: Government, Health, Science, Education, Culture and art (Smolenski, 2017).

According to the above principle, existing Blockchain applications are still at 1.0 and 2.0 levels. Most people even do not aware of the "blockchain" to name possible uses of blockchain. Although researchers have discussed the commercial use of the blockchain, several chainchain technologies can be used in education (Mamoria, 2017).

1.1 Problem Statement

In response to the increase in the demand for education, we can also talk about the increase in the number of institutions that respond to these demands. Correspondingly, as the numbers and possibilities increase, the diversity of the channels in which the training takes place increases. Considering that most of the existing information systems and work flows involve manpower and bureaucratic processes, we can find it doubtful that it will meet the needs that will arise as a result of diversity and volume increase.

Educational institutions accept student applications for the programs they offer. Subsequently, when the student reaches the determined educational objectives

related to the related education, the student is prepared and certified with a certificate or diploma of his own. These success and completion information are stored in information systems or physical documents of educational institutions. Again, the reliability and verifiability of this information is monopolized by the relevant educational institutions. Even though a copy of these documents has been given to the student, a number of work flows are resorted to the authority of the institution. An example of this is the process initiated for a course that was previously taken (course exemption).

When we consider not only educational institutions such as well-established universities, but also the internet initiatives that provide online education and small-scale language schools, the reliability of the information systems of the relevant institutions and the accessibility of the information (especially when the institution closes) can be at risk.

Another risk is the data fraud and imitations that can be made in the data of these institutions after the registration of the documents given. This situation is within the scope of stealing the corporate identity of the institution and to overcome this, many of the document holders use sources such as notary public.

The point that makes the work flows related to the education history of the people dependent on the bureaucracy is that the educational institutions' own information systemts that hold the educational content and student information are not digitally portable and shareable. Therefore, the information systems of the relevant institutions lagged behind the online technologies and due to the reliability and integration problems, they still need many workflows related to physical documents and manpower.

In the current situation, students can only be included in a program under an educational institution and can use the educational resources of that institution. If they

do not provide educational content related to the field they want to specialize in the program they are enrolled in, they cannot create alternatives to themselves and they are most likely to wait for the institutions to initiate bureaucratic processes for the courses they will take from different faculties.

1.2 Aim of the Study

Courses and certifications are offered by various organizations such as schools, institutes, private initiatives, etc. As the number of organizations and programmes are increasing, more advanced learning and specialization paths become available.

This study aims to build a decentralized and trusted information system that ensures the longevity, interoperability and verificability of all course data and individuals' completion progress.

With the help of the particular technology in education, it aims to create new opportunities and to contribute to learning.

1.2.1 Research Questions

This study tries to find answers to the following research questions:

1. What are the necessary properties of authentication system of online student profiles on a blockchain?
2. How can the entire educational background of individuals be kept in electronic environment without the need for third party authorities, ensuring the reliability, verifiable and persistent data?
3. How can the exchange of student information be provided without the need for any central authority?
4. How is it possible to ensure that those who wish to receive education are not limited to the educator resource under the roof of any institution, but use all the educational resources included in a system and create an education path with them?

1.3 Significance of the Study

In terms of trust, blockchain technology can change the way people build trust by building it up through third-party vendors and building it through technology. The behavior of teachers and students is recorded and monitored when Smart Contract and Blockchain are applied. The trust between the subjects is based on the technology itself, not the third party.

Equality refers to the same rights and opportunities that everyone has in a blockchain network. The openness, boundless, and unauthorized nature of Blockchain technology can provide everyone with equal access to the technology and its associated network. Anyone can apply for an electronic purse on the Blockchain network. Blockchain technology puts no limits on users. Anyone can use it on a daily basis, avoiding authority priorities.

Just knowing the identity of the parties in a transaction would mean that third parties should have complete confidence in the company. Since these circumstances are rare, it is also necessary to have confidence in the release of the certificates, in particular by presenting the methodology with which the Issuer reaches ared the conclusion referred to in the claim.

Decentralization of academic information chain without having trust and security issues potentially enables new facilities. The study will also be looking to reveal these positive outcomes.

1.4 Definition of Terms

Education technology, innovative forms and assets through the production, use and management of the development of education to advance the Honor and principle of the insistence on knowing (Januszewski and Molenda, 2013).

Blockchain is a distributed record innovation (Smolenski, 2017) that uses cryptographic methods and common contract calculations to create the highlights of

decentralization, traceability, persistence and monetary features. Web, "open, web-based, standards-based interface creation with independent, secluded trade practices" serves as. It focuses mainly on scores and compliance with web measures (Alonso et al. (2004).

Certificates restrict the ability to create new educational pathways, especially for those who do not have access and need most of the time, to monitor and up-to-date registration systems. For people who do not have formal education, the challenge is to turn their learning into jobs, because they usually have no references to verifying their skills and experiences (Schmidt, 2017).

E-learning refers to the use of internet technologies to provide a wide range of solutions that enhance knowledge and performance (Rosenberg, 2001).

Learning Management System (LMS) is an approach that has potential and important concepts in computer use in education, but is often misunderstood and abused (Watson et al., 2007).

Chapter 2

LITERATURE REVIEW

This section explains the concepts of online education, blockchain technology, its certification and summarizes the related studies.

2.1 Online Education

Online learning today is the newest and most popular form of remote learning. Over the past decade, this has had a significant impact on post-secondary education and the trend is increasing. Online education, defined as a platform for providing educational content and facilitating interaction between teachers and students through a computer network, has grown rapidly in the 1990s over the next decade. In the same period, increased demands for accountability in higher education led to the development of measures to determine the value of higher education in general, called learning outcomes assessment (LOA). In addition to historical proximity, these movements - online training and Loa -. This was an important aspect: both the introduction of destructive concepts in traditional classroom teaching and faculty-centred teaching, and the effectiveness of traditional teaching and learning models that have remained unchanged for centuries (Oakes, 2002).

In most cases, the two movements developed independently. Early education and training studies focused on traditional classroom teaching or teaching. Online courses have only been decided whether learning outcomes are face-to-face standards. Even today, Loa's efforts tend to use the same approach. Ask the same questions face-to-face against classes, online classes. What has not yet emerged is a more complex

understanding of the possibilities of online learning to change the way we view, design and manage Loa programs (EDUCAUSE, 2003).

There is online training because technology made it possible. Technology also provides an increased ability to track, assess, and respond to student behavior and mastery in online courses at depth and speed more than ever before. Researchers focus on a large number of student data that can be collected and archived in online courses and programs to "win" data to help students improve learning outcomes. These approaches, known as "learning analysis" in higher education, enable teachers and course designers to rapidly change their teaching practices and curriculum. This enables students to make informed decisions about learning behavior and course selection. Developing technologies also revived powerful teaching methods, such as mastery learning, decades ago, with the development of online education in some cases (Stiehl and Lewchuk, 2005).

These technological advances have the potential to revive the traditional and online education of Loa. Although efforts at LOA have increased significantly over the past 10 years, most institutions have used evaluation results to reduce accreditation pressure rather than to improve students ' learning. The pressure of the public and the federal government to consider the results of higher education no longer allows us to provide lip support for students to learn. The promise to assess learning outcomes is that continual improvement of curricula and instruction should improve learning performance for all students. Online education and related technologies offer better opportunities for all students to achieve their full potential (Palloff and Pratt, 2009).

2.1.1 History of Online Education

Online learning is asynchronous or synchronous, or a combination of both. While asynchronous learning means non-synchronous teaching and learning, synchronous learning refers to teaching and learning simultaneously, both

technologies and over the internet. Online training 20. since it began at the end of the century, most online programs and courses were synchronized using instant messaging and text messaging. Chat rooms and instant messaging allow users to decide who is chatting simultaneously (Technavio, 2017).

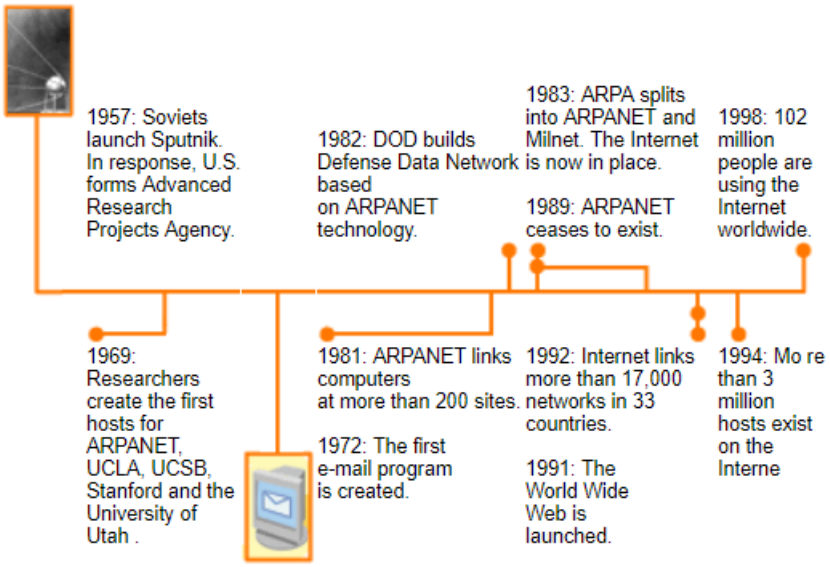


Figure 1. Historical background of the internet (sabri.org)

The invention of the @ symbol for use in e-mails in 1972 and the emergence of the World Wide Web (www) in 1991 to connect to the internet have become the latest online training. The universal use of websites offers opportunities for the development of online communities and groups. Email, Conference, chats, work with Google Drive, Doc, Hangout, Dropbox, Facebook, Twitter, etc. It is widely used in online classes (Cormier and Siemens, 2010). Online training can be categorized by users. These are (Rodriguez, 2012):

- Online, university-level education, which is individuals registered to receive degrees and diplomas at universities;

- MOOC (Massively Open Online Course) that motivate users to motivate themselves as individuals motivated by learning goals, background information, skills and similar interests (also called major open open online classes).

In general, students in the United States register to universities that have extended their existing classes in online course formats. These facilities usually offer two types of online courses - full online courses (not taught in tuition classes) and mixed / mixed courses (a combination of existance and web-based and technology-driven formats). Students in these two online modes gain points, degrees and credentials when they complete the required courses and internships.

MOOC (Massive Open Online Course), which includes online services for universities and companies, was introduced in 2008 in order to improve access to higher education for larger segments of the population. The University proposal was initiated by edX 2012 from Harvard University and edX 2012 from the Massachusetts Institute of Technology (MIT), eduMOOC 2011 from the University of Illinois Springfield, five partner universities (Princeton), Stanford Califonia / Berkeley University (Princeton), Michigan-Ann Arbor and Pennsylvania, etc. Many of them are open to the public. This reflects the universities ' efforts to ensure public participation in online education. Corporate-based online offers, whether free or non-profit, are primarily launched by organizations, businesses and individuals. After retiring from Stanford University in 2011, Sebastian Thrun launched a non-profit online venture, Udacity. According to the website, Udacity offers a number of certificate options that are recognized by major technology companies that are active within the student body. Peer 2 peer University (P2P) is an online educational resource conducted by volunteers who teach all courses. According to websites https://www.p2pu.org/en/) public, "not

only helps students to take an online course, but also higher retention rates than most online learning courses."

Founded by the Saylor Foundation in 2008 Saylor.org it is a collection of high-level courses that are open to the public and free of charge. According to Web sites, Saylor.org not the Academy; “it is based not only on open education resources and open-source learning technologies but also on open access to qualifications and continuous open learning opportunities” (Glance, 2013).

2.1.2 Definition of Online Education

Online education is the creation and dissemination of personal computers, globalisation of ideas and other human actions, and sharing of ideas and use of technology to access more people. Audio, video, computer and network technologies are often combined to create a versatile teaching system. The main way to connect a remote teacher with a student is the network. Networks suitable for remote applications include satellite, cable modems, digital subscriber lines (DSL), and wireless cables (Collins, 2002).

Greenberg (1998) defines contemporary distance education as “a planned teaching / learning experience using a wide range of technology to help students achieve distance learning and improve interaction with learners and learning certification.

Teaster and Blieszner (1999): “the term distance education has been applied to many teaching methods., however, the main difference is that the teacher and the student are spatial and probably temporarily separate.”

Keegan (1995) offers another definition. It states that distance education and teaching is the result of technological separation between the teacher and the student, which saves the student from having to go to a fixed place at a fixed time to meet a

sound person to be trained). From these definitions, we can see that the student and teacher are separated by space, but not necessarily in time.

There are many terms for online training. Some of them are virtual education, internet-based education, web-based education, and computer-aided communication. The web edu project uses an online education definition based on the definition of Keegan (1995). This is:

- Separation of teachers and students from teaching education,
- Effect of an educational institution separating it from individual work and private lessons,
- Using a computer network to deliver or distribute educational content,
- Provide bi-directional communication over a computer network.; thus, students can benefit from communicating with each other with teachers and staff.

2.2 Blockchain Technology

“Blockchain” is becoming a part of the technology. In simple terms, a blockchain is a distributed book that can be used to save and share information from a community. In this community, each member keeps its own copy of the information, and all members must review all updates together.

Information, transactions, contracts, assets, identities or virtually anything that can be digitally defined. Entries are permanent, transparent and searchable; this allows members of the community to fully view the process history. Each update is appended as a last “block” of the "chain". Blockages have been tried since the early 1990s, but until 2008, blockchains could not be spread by publishing a White Book by name of Satoshi Nakamoto. The first known blockchain is the Bitcoin, a decentralized encrypted electronic currency. Bitcoin is also a name for the underlying the network protocol of the electronic currency. In common speaking language, other blockages

such as Bitcoin blockchain and Ethereum Blockchain are automatically assigned to blockchain when they are of great importance in practice.

2.2.1 Ledgers

Ledgers are tools that, can be used to manage the ownership of an asset. They maintain a list of transactions to follow owner information of assets.

TRANSACTION NO.	DATE & TIME	SENDER	ASSET	RECEIVER
#	dd-mm-yy hh:mm	Person 1	Description of asset transfered e.g. a unit of currency, a deed toa property or a certificate.	Person 2
#	dd-mm-yy hh:mm	Person 1	Description of asset transfered e.g. a unit of currency, a deed toa property or a certificate.	Person 2

Figure 2. A sample ledger content (Newman, 2017)

Ledger is also a commissioned list of asset transactions makes systematic capital transfer and accumulation possible and is therefore defined as the basic technology that makes capitalism possible.

A person or organization possess of a physical control on a public ledger has significant impact and power. In particular, owner of ledger (Peters & Panayi, 2016):

- Decide whether to record a transaction that gives that person the option,
- Set conditions for peers to record their transactions,
- Decision on the control system to verify the accuracy of these transactions.
    - Modify the history of transactions already contained in the general ledger,
    - Shutdown or corrupt the general ledger completely.

In such a system, altering the history of transactions in it also allows the modification of asset ownership. The person or organization controlling these accounts has a significant influence on who owns them - only as responsible for the transaction list - effectively controlling them.

2.2.2 Blockchains as Public Ledger

The first known blockchain protocol is Bitcoin's blockchain protocol. In this protocol, the hash of public keys is simply used as an address. The addresses have some special rules that start with “1” or “3” and must be fixed length. Addresses in blockchain protocols are public keys. In asymmetric key cryptography, direct relative public key and private keys are used to sign any file. As the name implies, public key can be shared publicly. It works just like the mail address to get mail. The private key opens the unique corresponding mailbox, such as the same key. In encryption, the sender encrypts a file to send and the recipient with a public-private key pair receives the encrypted file and decrypts it with his private key. If a file is encrypted with a public key, the unique key to decrypt is a private key. This is the traditional use of public-private keys in cryptography. In distributed accounting technologies, it is important to prove who the signer is to create a reliable environment without a central authority. To do this, we use public key cryptography. In the blockchain protocol, each node has its own public and private keys. When the node creates a process, it signs the process with its own private key and broadcasts the process to the P2P network. After this process, the network has a process that is signed with a public key, which means that the owner of the private key is used to sign the process. If the signature is signed with a private pair of the public key, the process is assumed to be owned by the public key owner. (Allen, 2016; Smolenski, 2016)

This mechanism allows us to use a public key as an address in the protocol. To illustrate the mechanism in a simple example, let's follow a basic scenario to see how

a process signature algorithm works. Suppose Alice wants to send Bob $ 50 and has created a transaction object and signed it with his private key. Then he broadcasts it on the network. A node that listens for broadcasts on the network captures the process. He can easily understand if it's signed by Alice.In this scenario, we do not hide transaction information from the network. Although blockchain operations are transparent, they are extremely durable. Public key encryption mechanism also provides anonymity. Using public keys as an address for the network address sent to the address which is knows how. However, the information that is the owner of the address is no longer shared. This mechanism allows us to solve the defining problem that has been solved by the central authority in the traditional money transfer scenario. (Gupta, 2017)

Since their function is to store transactions, all blocks have a electronic currency that is traditionally considered to be the most basic asset dealt with over the network. This also encouraged the introduction of this blockchain by paying participants in their own encrypted currencies. Blockchains are therefore books that contain groups of operations (also called blocks) that are encrypted in a linear chronological order. Other key characteristics of a blockchain are security, invariability, programmability. (Smolenski, 2016)

2.2.3 Blockchain in Aspect of Social Values

When dealing with a topic like blockchain, initially there is a tendency to focus on problems related to digital disruptions, the digital economy and the information. However, more than just digital technology is often important: socio-economic factors that produce (or respond to) technology needs can be equally important or even more important. The most powerful digital business models first understood people and then digital technology. (Christensen & Clayton 2003)

2.2.3.1 Self-Sovereignty and Identity

Blockchain's first literature often refers to "autonomy" and the ability to take and control an individual's online identity. (Lilic, 2015)

Public blocks enable self-employment by controlling the access of personal information. In a pedagogical aspect, the term is synonymous with the ability to take, manage, and share the details of individual students ' competences without calling the educational institution a reliable facilitator.In addition, it may be considered citizens who have an important “self-management” about how personal data and identity are shared online and who have the opportunity to free them from access to the services they wish to provide to the third-party. This is data or identity. Identity is a complex area for citizens and those who need to examine it: an evaluation of personalized data with its history. Digital identity is limited to human rights.

2.2.3.2 Trust

An effective study by the UK Government reveals that, trust is a risk share between at least two people, organizations or states. Therefore, it is based on these requirements:

a) Authentication – checking the identity, answers the question “who”;
b) Authorization – checking the access, answers the question “is s/he allowed to do that”.

If one side is not satisfied with the other's answer, it may still choose to allow it, but to do so carries a risk. However, if the parties do not trust each other, there is no applicable relationship. In this sense, it is reliable to be trusted in a society.

This basic concept of trust still remains in the digitized life. Here, in good faith and in order to act for ourselves, we must rely on many actors that we will never encounter: trust is given only in a certain context and within a certain period of time for a specific practice. Digital economy’s trust challenges are are becoming more

complicated in terms of cost, efficiency and time. Hope is that the internet as well as blockages can re-create communication and affect social behaviour and help to close existing differences between processes, contracts and reliable foundations of business, government and society.

Accessibility and transparency are some of the key features of a blockchain. In the current system, the absence of one or the other functions is usually a fundamental driver for the acceptance of blockchains. They become especially critical when a large number of organizations engage in block entry. Blockages provide participants with information about the origin and ownership of each asset or record and how it changes in time.

However, observability only works if chain operations are associated with an id. Without the identity of the public, the code of the blockchain operations cannot be deciphered or traced to the linked document or serial numbers. In this way, it is also known as "global" blockchains - block blocks are special, but occasionally may be used to observe the processes of some targets through certain chain data. Blockchain has an undisputed methodology to validate that data exists at a specific time for a transaction. Because each block in the chain contains information about the previous block, the history, location, and ownership of each block are automatically verified and cannot be changed.

2.2.3.3 Immutability

Public key cryptographic algorithms emerged for the first time in the 1970s and revolutionized the world of cryptography. The requirement to share the key used in symmetric encryption algorithms from a secure channel before encryption was causing major problems in many usage scenarios. In particular, cryptography with public key has brought a solution to the encryption problem between participants who do not have such a secure channel. Public key algorithms consist of one public key

known by everyone and one secret key known only by owner. An encryption with a public key can only be decrypted with the stored key. The relationship between the public key and the secret key is based on difficult mathematical problems that are not possible in terms of computational power. RSA, ElGamal and NTRU can be shown as the most popular open-key cryptographic algorithms.

Public key cryptography is basically used for two purposes. The signature Key can be used to decrypt the key. In this type of use, the sender encrypts the message with the recipient's public key and the receiver decrypts the message with its own private key and obtains the message.

An entry in blockchain is made fixed and unchangeable on its creation. Since its hash prevents the changeability of the data, blockchains last state become constants. Additionally, copying the blockchain to multiple locations made this constancy irreversible. By encrypting with the asymmetric encryption keys, transaction security is ensured. This ensures that the data is not compromised in anyway and prevents unwanted data tinkering. For a transaction blocks to be marked as valid, the other peers, who share the same blocks, need to accept the validity.

The other area of use of asymmetric cryptography is the signing. Signing is used to check whether a message has actually arrived from that sender. The sender signs the message with its own secret key and sends it to the recipient. The receiver verifies this signature using the sender's public key. Verifying the signature ensures that the sender's identity is authentic.

In blockchain technology, the use of asymmetric cryptography can be listed as follows:

- Signing transactions with the stored key,
- Derivation of account addresses with public keys,
- Explicit verification of transactions signed with the stored key

2.2.3.4 Disintermediation

By trading with agents with Science, Blockchain can also get a few certainty. (Piscini and other., 2016) Members in a blockchain are connected to each other in a showcase where they can trade directly on the stock exchange without the assistance or mediation of third parties and change ownership of direct value-added resources. A respect, in absence of central authority, regulates things. With blockchain innovation, P2P agreement calculations can easily record and approve exchanges without requiring a third-party. This can reduce costs, delays, and overall complexity, or indeed reduce it.

2.2.4 Record Types in Blockchains

A blockchain can consist both transactions and smart contract definitions.

2.2.4.1 Transactions

Transactions is a question of expression in the most important way that a certain process is true from one side to another. Signatures are evidence that the notification has been made with these events.

There are three types of Resource Exchange records:

- Amount transferred in one currency: The value of the currency is unified and has the same reputation. What's more, monetary standards can be intra-converted over a commercial price. The most common form of money that benefits from blockchain innovation is Bitcoin.
- Proof of documentary property rights (deeds): The non-trivial property right ownership.
- Smart Contract Transactions: A transaction entry which is defined in smart contract’s definition.

2.2.4.2 Smart Contracts

Smart contracts are computer programs that are left in a chain of blocks running a trade under certain conditions. Then, a clever contract is a regular expression such as "change from X to Y in case of Z". It is not like a normal contract to which the parties sign the contract after signing it, but a clever contract is executed by itself. - once this has been established in a chain of enlightened blocks, there is no possibility of establishing conditions of compliance with the conditions naturally without the support of the stock market parties or other third parties.

The guarantee of conscious contracts is that in a situation where critical digital records of an industry are indisputable, the mechanization design of an unused biological design system will advance to form an unused social fabric that will strengthen bourgeois sufficiency, individual portability and regulatory change. Sharp contracts are therefore a long-standing robotic appearance in this context.

Certificates and Digital Signatures can be stored as smart contract transactions and needed to be defined in smart contracts. Smart contract interfaces can be used to store cryptographic abstracts of the certificate ("virtual fingerprints") or to store themselves for claims.

2.2.5 High-Level Architecture Overview

A blockchain can be a record of participating in consecutive "frames" of exchanges, (IBM, 2017):

- Anyone who wants to exchange a resource through a private or open arrangement must go to the organization. This occurs through a program application that interacts with the client and blockchain. The computer program application is regularly referred to as "wallet". In particular, it can be introduced in a gadget or acquired through a web browser. Depending on the plan, a wallet can be used to transfer advanced resources. While several hand

bags allow the exchange of coordinates without external intervening, other hand bags are operated by individual ends who hold users' advanced resources in their own name.

- Customers who need to deal with the approval of transactions by agreeing, big or big, introduced Blockchain program to their devices. This can be used to create a common record, make a duplication of the entire record, and store all copies of the record super synchronized. Hence open blockages enable everyone to promote the computer program and store a copy of the account receipt, everyone can exchange in particular within the blockchain within the edit and cannot force any third-party to require it. In approved blocks, a centralised expert decides who will come to the centre and deals with the negotiation process.
- Swap records or parts in a blockchain are cryptographically linked and protected from tampering. It is not possible to change or delete a change in the blockchain after the registration and timestamp, not just as the records in the changeable computer databases. The blockchain includes the reality of change, that is, how it has been exchanged, as well as the edited data on the exchange (metadata) and a cryptographic summary of the item of change ("enhanced unique fingerprint"). This private signature is then used to confirm the stock market: when someone changes the stock market, the arrival of a kind of code from someone in the chain does not match the version and the blockchain computer program emphasizes inconsistency.
- All parties involved in the stock market and those parties, as well as recently used to the organization by adding a stock market record must agree for a period of time. All other hubs within the scope of the arrangement have checked that the two sides have the appropriate capacity to take part in the

stock market. Therefore, one party decides to transmission and other one decide to reach the source, and the Centers confirm that both parties can collect the stock exchange.

- All computers in the arrangement control that the copy of the blockchain is unbroken and numerically indistinguishable from all other copies in the array. Most computer adaptations are expected to be "original", so the way to "hack" records is to check more than half of the computers in the organization.

2.3 Certification

In general, the certification shows any identifier to that a certificate is issued to confirm a request. However, it may be having various purposes in education:

- Learning outcomes in any case to achieve learning outcomes• proficiency of a teacher, regardless of the learning style,
- A learning preparation performed by a student,
- A teaching institution or course that meets a quality requirement,
- An accreditation agency is authorized to issue certificates.

Schmidt (2017) limits our capacity to make new teaching paths, especially for those who need them most and need them most. A challenge for individuals who do not have formal education is to convert what they have learned into hiring, because they have no references to confirm their abilities and encounters.In addition, the existing enrolment frameworks, in spite of the clear benefits of long-term instruction and casual and informal instruction, make it difficult to create important non-learning and non-professional training programs, and support formal teaching for other learning encounters.

Smolenski (2017), "talent, other characteristics - Polish, nationality, religious personality - it has become a transnational, intrigue flag for talents and talents in an

unacceptable environment." Accreditations help us identify individuals of a community with specific capabilities, as well as who can communicate information.

2.3.1 Components of a Certification

Certification is the other thing that is the sum of a certain reality after the receipt of components: to make a statement from one party to the truth. Therefore, each certification brings together (MIT Media, 2016);

- Explanation - "this set of realities is real". Cases in a teaching environment may be "a student has provided a capacity", "a teacher has sufficient knowledge to train", or "a learning performs a task".
- Support - an organ that confirms that the claim is true.
- Proof that the claim is supported as a rule, counting the method of review of the claim, and additional data to almost any part of the claim.
- The beneficiary - the individual required by the request - the learner who learns an ability, the instructor who has enough knowledge to teach, or the trainer who completes a task.
- A certificate - a report documenting the personality of the promoter, the quality of the promoter, the claim and the evidence in fundamental cases.
- The certificate contains a signature of the type of stamp, glyph or qr code that may be added by supporter, and therefore authenticates it.

2.3.2 Processes of Certification

The certification comprises three distinctive forms (Schmidt, 2015):

1. Issue: Usually the methodology for collecting the claim, the backer, the confirmation, the beneficiary and the signature on a certificate. Regularly this information is recorded on both in a central database and certificate’s itself.
2. Verification: Usually the methodology for confirmation of the actuality of the certificate.

a. Verification with security highlights joined within the certificate itself: this may incorporate measures such as confirmation of the realness of a seal, signature or etc.;
b. Verification of the certificate with the first backer, whereby the third-party contacts the first guarantor and inquires on the off chance that he has really issued the certificate;
c. Verification by comparison with a centralized database of claims.

3. Release: Usually the methodology for offering a certificate to a third-party.
   a. Direct transmission of the certificate (or a duplicate of the certificate) to the third-party, e.g. by mail or by appearing it to the third individual personally,
   b. Storage of the certificate at an overseer bank which may as it was share with certain people upon ask (eg within the case of a private will the public accountant is as it were entitled to share the will with the recipient after an individual) death),
   c. Publication of the certificate by setting it in an open enroll or shop where anybody can counsel it.

2.3.3 Standardized Processes for Issueing and Certification

Knowing personalities of peers in exchange considers mercilessly that third parties must have complete certainty within the company. Since these conditions are rare, it is essential to be certain about the discharge of certificates, especially by presenting the strategy for which the guarantor has reached the conclusion specified in the request. Moreover, all fees within a system must be guaranteed to be published in a typical and decent manner.

A certificate is issued to each individual as it meets a certain requirement. This also needs that the technique be archived to a standard that is followed by each

transmitter. If a certification framework contains a large number of issuers and applies individual or exclusive rules to issue each guarantor certificate, the inevitable result is the creation of a large number of subsystems. They must be captured and approved independently and autonomously to create faith.

2.3.3.1 Mechanisms for Regulation and Security

Once a standard certificate framework is created, it is necessary to believe that each of the parties in the framework will act with great confidence and implement the appropriate criteria for their needs. For this reason, a certification framework that includes a component that confirms that the parties act with great confidence and that the parties that do not do so remove (and discharge) the mask will result in greater certainty in the overall framework. These tools (Certificates.media.mit.edu):

2.3.3.1.1 Security Features

A third-party who wants to confirm the claim on the certificate must validate that the certificate is not fraudulent. To list some ways to predict such counterfeit products:

- By means of physical destructive components, such as brands, watermarks and unusual plans, the certificate can co-ordinate into itself, guarantee that it can carry out this specific certification as it supports;
- Compensation by a database maintained by a guarantor or by a central database, so that a third-party can validate.

2.3.3.1.2 Accessibility

The final component of believe in a certificate is that the claim is effectively open. As a result of this:

- The beneficiary of the certificate ought to be able to keep a duplicate of the certificate.
- Third-parties who need to get the certificate ought to effectively get it from

either the proprietor, the backer or a register,

- The certificate ought to contain data on how to confirm the claim and what measures and forms are utilized to claim and issue the certificate,
- The data within the certificate ought to be clear, lucid and simple to utilize. This includes:
    - Standardization of the substance of the certificate itself,
    - Make beyond any doubt that the certificate is machine-readable.

2.3.4 Use of Certification in Education

Certification is used in various use cases for educational purposes. These use cases can be divided into two main categories by their targets.

2.3.4.1 Use of Certificates for Learners

Certificates are used for all purposes. As a work of the show, certificates are issued to students:

- Complete a specific learning challenge. Examples of this may include the following: high school recognition of non-formal education in co-operation / support experience certificate or versatility certificate,
- Sum of learning in a particular field, document the representation of scholastic achievement in higher education through the granting of ECTS credits learning objectives through the realization of specific discrete learning units,
- Private encounters that contribute to learning, for example: a certificate of completion of apprenticeship or other work experience,
- Securing special skills. For example, by issuing certificates in approval strategies for pre-acquired information,
- Fulfillment of certain brightness criteria in cases of gaining certain grants or graduating with honors for Success,
- Special qualification obtained by issuing certificates or course cards at regular

intervals.

As a work of the show, the certificates given to students are used by partners who are interested in showing a person's learning. For example, instructive training is fascinated by deciding whether a person is eligible to go to another instructive level. Record professionals and potential bosses are enthralled by deciding whether a candidate is reasonable for open business opportunities. In addition, literature refers to the use of certificates as a stimulating tool in teaching. That so, learning through certification to achieve specific learning objectives. (Gibson et al, 2015)

These progressive developmental evaluation steps have been shown to provide learning outcomes.

2.3.4.2 Use of Certificates for Accreditation

Accreditation may be a formally recognized sap that an important organization or individual has the ability to perform certain tasks. (ISO / IEC 18009: 1999) Accreditation as a certified rule with a certificate. Several forms of accreditation in recruitment work: education institutions have been licensed to be authorized to work. Examples of such accreditations are the accreditations of governments in colleges or schools.; accreditations on central preparation for teaching specific computer program packages by program companies:

- Certification of specific teaching programs in recognized teaching institutions,
- Instructors regularly certify specific capacities to claim to be trainers and train specific schools,
- Accredited institutions that certify schools and trainers themselves are authorized by high-level controllers guaranteeing authority to set rules.

Most of these accreditations are regularly placed in the accreditation chain. For example, a consultant may have received a certificate of completion for a certification program issued by an authorized college authorized by a licensed quality approval

organization. The flow shown in Figure 3 is an example of such accreditation structure where high European directives are normal.

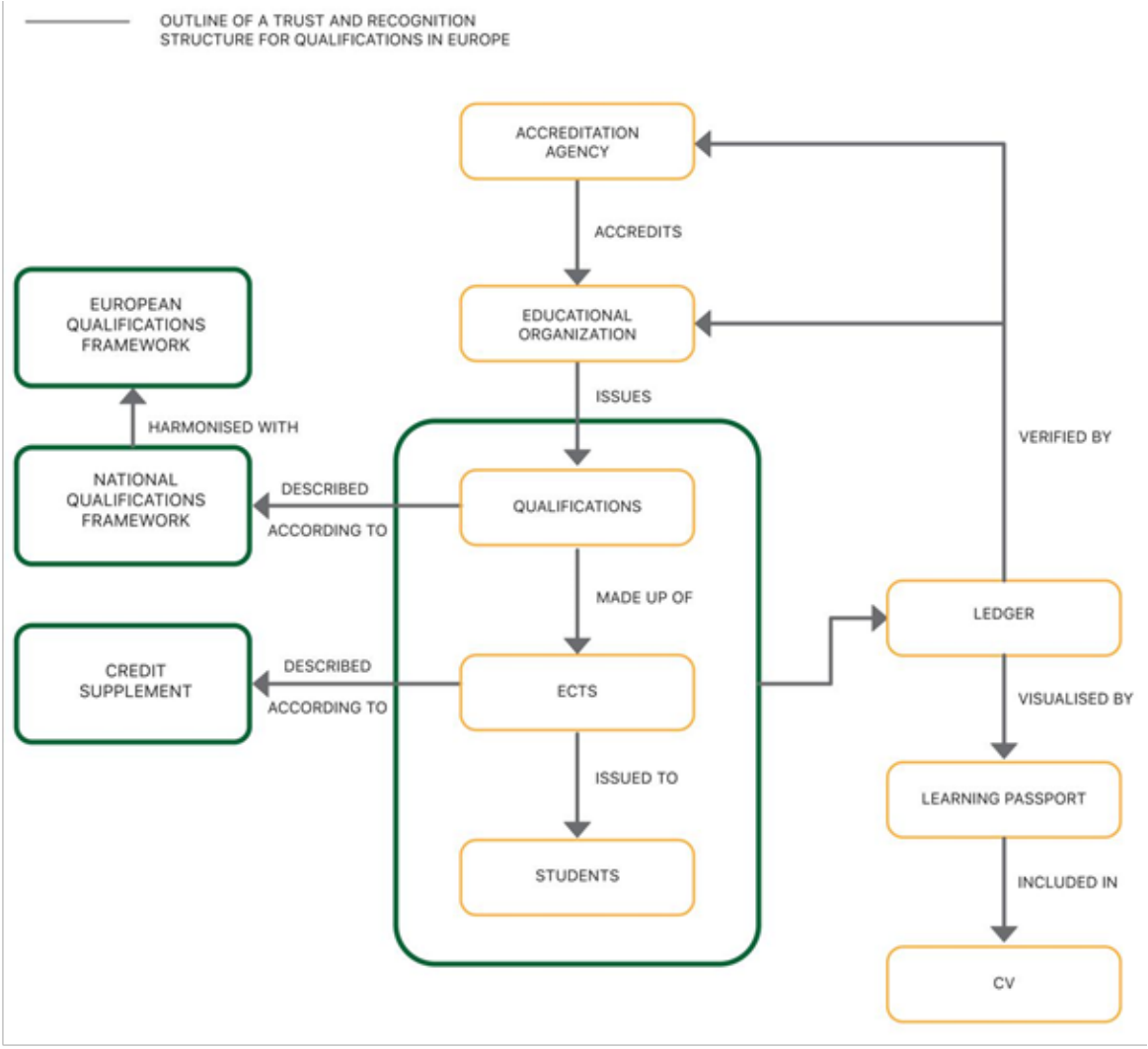


Figure 3. A sample trust & recognition flow (Camilleri, 2017)

2.3.5 Use of Intellectual Property Tracking Certificatesik

Registration of mental property can be a central component of all scientific and monitoring system. Intellectual property respects and can lead to costs of exploitation. To reach this conclusion, a large number of Central experts are used to control the mental property of various types:

- Research logs confirm that the research group has not been used in which the

research is agreed in accordance with a comprehensive logical standard,

- This data is used to make logical decisions,
- Data companies confirm how often a research is stylized or the explicit instructional informative resource (OER).

This, it is often used regularly to decide the importance of research on OER and to make up for the creator accordingly. Patent employers certify the primary creator of a development and monopolize them for a long time to demonstrate and gain advantage from this invention.

2.3.6 Use of Financial Certificates

Certificates are too broadly utilized for money related reasons, such as; payment, schoolships, student loans, etc.

2.3.7 Limitations of Certificates

Most of the records are published on paper, despite the progress of the digitization efforts of governments and businesses around the world. (Cheng et al., 2016)

Since most of the countries do not completely issue certificates digitally, there is no “idealized organization”. Critical barriers to each framework clearly demonstrate that superior and stronger certification innovation is required.

2.3.7.1 Limitations of Paper Certificates

Physical certificates are most trusted framework in many countries. Certificates are difficult to fake because of security incidents in itself;

- (usually) straightforwardly from the beneficiary, who hence has full control over his certificate;
- Reliable capacity for moderately long periods,
- They can be displayed by the beneficiary anyplace, for any individual for any purpose.

Nevertheless, these certificates have notable weaknesses: although it is difficult to counterfeit, no certificate is not tamper-proof. The issuer must then maintain a central certificate list that can be used to verify the authenticity of the certificate. The certificate is a single source of error;

- Registration of such a claim and replying questions about the validity of certificates can be a manual path that needs human effort;
- Security incidents in the physical certificate are based only on the level of challenge and ability to create the record.
- How secure the certificate is, it's so expensive to produce.
- There is no limitation on the capacity of the participant to dishonest the timestamp or other subtle elements of the certificate.
- Once, there is no flow of rejecting the certificate unless checking the details manually.
- Certificates are used by a third-party, e.g. To confirm requests in a resume, each certificate must be examined and approved physically only.

2.3.7.2 Limitations of Non-Blockchain Certificates

Non-blockchain certificates have numerous interests on paper certificates: they require a lot less assets for efficiency, support and use because:

- Authenticity of certificates can be controlled naturally and isolated from human interaction,
- If a third-party is required to use certificates, they may be compiled, certified and actually combined.
- Certificate security is cheap to issue the certificate; however, it depends on the security of cryptographic contracts that guarantee that replicating by anyone other than the issuer is surprisingly costly.

Certificates can be rejected by the participant, some support extenders depending on the framework's plan. As can be, computer certificates have critical barriers, so it is surprisingly easy to fake without taking advantage of advanced signs.

- If advanced brands are used, request the evaluation of third-party certification suppliers to ensure that the transaction is evaluated,
- These third parties have critical control over each certification and approval arm perspective that could be exploited,
- Since there is no global standard adopted for computerized signs; this leads to certificates that can only be validated within certain computer program ecosystems,
- Electronic records are less difficult to destroy - you want to use fault tolerant modern multilevel reinforcement frames to ensure that they are safe,
- If the registry remains inadequate, the certificates themselves become useless because they don't like paper certificates that they don't respect naturally without registration,

2.4 Digital Certificates with Blockchain

Blockchain is ideal as a new platform for securing, sharing, verifying learning outcomes. (Smolenski, 2016)

For certificates, a blockchain can contain the details of each certificate's transmitter and receiver. These details are stored the same way on grid of computation resource world-wide, along with the document's signature (hash). Thus, digital certificates attached to a blockchain have significant advantages over "normal" digital certificates:

- It can’t be imitated because the certificate can be issued and received by persons specified in the original document.
- Certificate verification can be done by anyone with access to blockchain, an

open source software that can be easily provided. - no agent party is required;

- Because no agent party has to approve the certificate. Even if the issuing organization or the output record is inaccessible, the certificate may still be verified.
- The registered certificates on a blockchain can only be destroyed if all copies of consisting blocks are destroyed.
- Hash is a checksum of a document originally has own identity. It is used to link between records and checking integrity of data. Blockchain records mostly use hashes as signatures, thus, it enables confidentiality of the related blocks.

2.4.1 Ideal Properties for the Recipient

Some quality requirements are expected to be satisfied for recipient's certificates. These are:

- **Independence:** The receiver achieves the information, and after that, it does not rerequire the issuer, or an independent party to be associated.
- **Property:** The receiver can prove that it's the owner of the credentials.
- **Control:** The receiver can decide how he handles them.
- **Verifiability:** Upon request the proof can be given by any third party, such as organisations that verify.
- **Permanence:** Each permission can be considered as eternal.

2.4.2 Ideal Properties for the Issuer

Blockchains is handled after obtaining the perfect requirements for a certificate for a participant:

- Supporter can show that the right holder has granted his / her consent,
- The guarantor can set the Expiration Time for the credential.
- The guarantor may refuse credentials. The authorization framework is secure and requires it to be negligible for continuous installation.

2.4.3 Other Properties

In order to ensure that the actual identity is valuable, a third-party validator can get the credentials as portion of an application. So, this validator is the authority that guaranties the validity of certification. The requirements for the validator are so:

- **Integrity:** The material was not controlled. To ensure the integrity, this is being compared with the exhibitor's original intention.
- **Authenticity:** The guarantor is to ensure that the certificate is not tinkered with.

2.4.4 Certify Identity with a Blockchain

In a particular perspective, a person's personality is a whole with fully identifiable data (PII). If it is necessary to verify an individual's personality with another person or organization, it shares it with a myriad of identifiable data. Therefore, for the purpose of representation, a planned expert can confirm his / her personality, title, address, government proof number, gender and grades in a distinctive manner to a college approval office. As a work of the show, the declarations office will store all this information in a central database, ensuring that the customer is virtually concerned about the security of his or her information. In any case, due to the respect of such information, false information, such as the emergence of a massive robbery by governments and organizations around the world, is powerless against such dangers as extortion and theft. Currently, when a person has to work with an unused person or organization, they must submit their information and allow someone else's control on the information.

Blockchain innovation strengthens the concept of an unused autonomous character that a customer stores personal data on a device. When needed, the personal data can be transferred. Regardless, blockchain can only allow verification of data by limiting the reading or sharing the all details.

2.4.5 Use a Certified, Autocratic Identity

When an individual has a fully self-contained personality (Gupta, 2017):

- Your individual data is carefully placed on a device, such as having and controlling the following: whether or not this information is a mix, allegation or computerized record; and whether or not this information is verified by third parties, e.g., by a third-party.
- An organization that publishes or approves certificates, along with other individual information, to a secure gadget; its mixed on a blockchain.

In the event that an electronic signatory or the party relying on the electronic signature suffers losses due to engaging in civil activities on the basis of the electronic signature verified by an electronic verification service, the party relying on the Electronic Verification Service shall bear the cost of the said Electronic Verification Service.

2.5 Issuing the Certification with Digital Signatures

A computer signature framework is used to issue certificates in all computerized certificate layouts. An advanced signature, an electronic signature routine is basically plotted on the archive.

- Sign a record with a timestamp,
- Do not doubt that the record cannot be checked after signing. For subsequent grades to work, they must have a personality number (public key) and a linked secret keyword (private key) for each person who signs a document.

2.5.1 Contents of a Digital Signature

An advanced signature comprises of these components:

- SHA-256 hashed content,
- public encryption key,

- private encryption key,
- timestamp.

2.5.2 Signing Documents with Digital Signature

A summary of a report is marked by combining the hash of an archive with a signature. This signature may be a combination of private key and a timestamp. So, the following applies:

- It is a type of signature for this specific record because it is made from a document hash, as it is done by the person requesting the private key. This note should be taken: since the signature is engraved in the advanced record, the "signed" advanced report contains a more distinctive complexity value than the unsigned advanced document.
- If a single letter of the archive is changed after it has been marked in an archive, the integrity will be broken.

2.5.3 Validating Digital Signatures

When a third-party has signed record, it must have the public key to decrypt the document. Since public keys are simply contains identification, they may be more frequent than not looking at open records in comparison with telephone contacts. The verification process checks the validity of signature for the document.

Certificate authorities (CA) also is used to establish trust between parties. Certificate authorities manages the trust centrally by:

- Enabling the connected asymmetric keys,
- Checking the timestamp,
- Executing the confirmation software,

Usually, the CA injects set of metadata in a certificate to achieve:

- Certification experts can confirm the identity of the people to whom the keys are issued, so that they can connect the public keys with the original IDs,

- "Watch" is controlled by the certification authority, so everyone can depend on brand history. As it should be, public key frames also make a central control and a point of blame. The consent program of the CA (e.g. bankruptcy, riot, restructuring, etc.).

Closing all marked reports declines most clearly. This is a critical issue for certificates such as birth, marriage or instruction that must end in a lifetime.

2.6 Blockchain-Secured Digital Certificates

2.6.1 Advantages

Blockchain innovation is perfect as a modern foundation for securing, sharing and approving learning outcomes. (Smolenski, 2016)

Public Key Infrastructure (PKI) replaces the central expert with proper alternative. This decentralized structure increases the life of the arrangement because there are a wide variety of copies of the frames in which the marks are placed. The decentralization of the blockchain has another advantage, because no third-party trader can change or delete the stock exchange left in the parts without fixing the request for confirmation. Beyond the limit of not trusting a CA or a trusted third-party, blockchains provides significant security benefits by providing a free timestamp.

A definite timestamp is mandatory in the event of a clear termination of the accreditations, but it is mandatory for a practical reason. The supporter should rotate the security key occasionally as part of the best security options, but make it simpler in response to a fundamental shortage. An autonomous timestamp information is required by a specific supporter to decide that the record is issued by a particular supporter when the key is important. Unlike many PKI frames, signs on a blockchain are also the autonomy of Registration Regulation: the same computer program can be used to sign any record type in any of the (restrictive) measures. (Thompson, 2017)

2.6.2 Architecture

Considering the certificates, blockchain consists of the certificate entries and recipients in an open database (blockchain), which imposes the signature (hash) of the document in an open database (blockchain) worldwide. Schmidt (2017) provides a certificate that uses square profits as a basic process in general:

- An advanced registration is made with several important data: the names of the distributor and the promoter, the date of publication, the credentials issued to accept open IMS competencies and soon.
- At this point, the supporter marks the certificate document encrypted with asymmetric key as the supporter receives.
- The guarantor adds this signature to the certificate itself.
- The guarantor makes an encrypted summary of the registration record - a short sequence of alphanumerics. That may be useful for confirming that the certificated is received by anyone.

There is a combination of alphanumerics that can be considered exactly like an advanced record, and any changes to the record give a mixed result. Lastly, the supporter who wants to record our certificate transaction with the receiver and date information, makes a transaction to record such activity. This supporter uses his private key to record our activity. The difference of alphanumerics on each party is shown in Figure 4.

ISSUER OF CERTIFICATE	HASH / DOCUMENT SIGNATURE	RECEIVER OF CERTIFICATE
1CytUYMWr439wms5MYjryCg5uM-sEhNHYW7	1b3793716c610c1a521d71b2f52c37e4c435d4cd990247ac0cd90a093f5d8fc8	1EUGqyEHbzGQ7hpvkPwm4XJG-FXC3duFvAn
1LSQXVvokuvBfRQUf8Q3rdkhVajK-gwHqoZ	d2bddd4516dd51e617fbb575a8384a1444a009b86d8d5c2440a28ed8d2db3790	1CytUYMWr439wms5MYjryCg5uM-sEhNHYW7
1b3793716c610c1a521d71b2f52c37e4c435d4cd990247ac0cd90a093f5d8fc8	1b3793716c610c1a521d71b2f52c37e4c435d4cd990247ac0cd90a093f5d8fc8	1b3793716c610c1a521d71b2f52c37e4c435d4cd990247ac0cd90a093f5d8fc8

Figure 4. Digitally signed documents in a blockchain (Schmidt, 2017)

Users' stored keys are of great importance. For the safety of digital assets, this key must be stored very securely. Applications where these keys are stored are called wallets. These wallets can be on local disks, while they can be in the cloud. Users usually don't have to do anything manual about hiding these keys. When creating an account address with wallet applications, these transactions are done automatically and the generated key is stored securely. Wallets also show the open key and the user's digital asset information.

The verification is done by comparing the hash of the record to be approved and the freely recorded hash of the blockchain. If coordinated, the archive is original. What's more, it means that anyone who receives a certificate marked in a blockchain can actually confirm the authenticity of the certificate if the editor is no longer available. If a real blue (or special) blockchain is used, it may, as well as individuals who have to reach a specific organization, signal, or approve this chain.

A sample blockchain-secured certificate issue flow is shown in Figure 5.

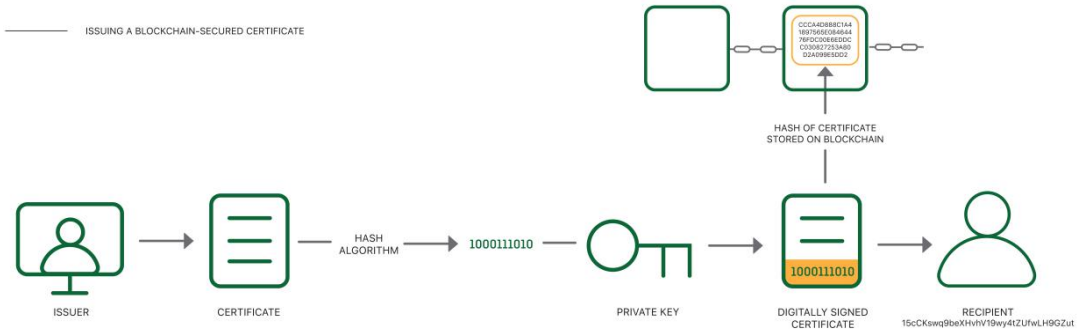


Figure 5. Issuing a blockchain-secured certificate (Schmidt, 2017)

2.6.3 Certification of Self-Sovereignty

Ought to a third-party ought to affirm that the information of an individual is genuine, they would have to:

- Person who offers the information in question,
- Prove that this information is true.

After confirming the information, the third-party seem at that point issue a certificate affirming the data as genuine, with an articulation. When this articulation is transferred to a blockchain, it gives an open affirmation that the identity subtle elements of the individual are genuine, without having to reveal data almost the individual in expansion to their public key.

A sample flow of blockchain-secured self-sovereignty architecture is shown in Figure 6.

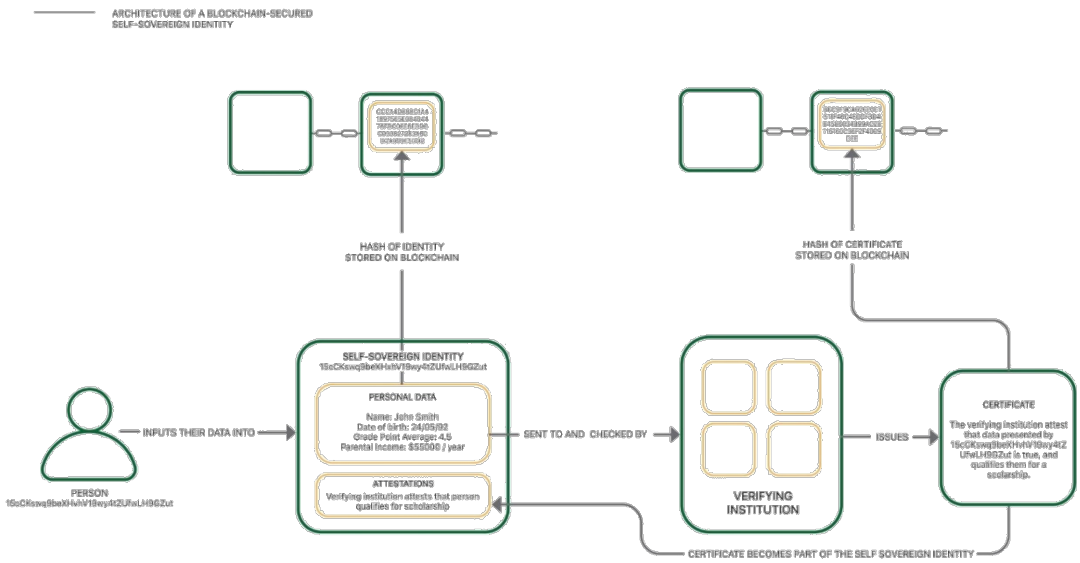


Figure 6. A blockchain-secured self-sovereignty architecture (Grech & Alex, 2017)

2.7 Use Cases for Blockchain Technology in Education

2.7.1 Open University (UK)

Open University is the driver vendor that provides UK learning analytics. As part of blockchain asking questions and accrediting, Knowledge Media Institute (KMI) is particularly interested in improving the internet publicity, certification and reputation criteria by using blockchain as a reliable registration. In addition to teacher involvement, it was normal to put open identities inside blockchain, and it was normal to do research on micro-accreditations and e-portfolios. By taking advantage of the accreditation potential to transform Ethereum's definitions into sharp contracts, KMI has created a model to collect and publish credentials in a blockchain. Omi offers KMI an opportunity to honor and inform all OU courses in blockchain. KMI's blockchaining technique is fully covered, and it empowers analysts to explore the limited potential of innovation at a specific angle (such as cryptography).

For the case, online learning requests less questions to be answered by putting the essence of meetings in a blockchain. For example, data that are about to be removed from a single learner can be made accessible to an outside analyst of student's studies to encourage a much better understanding of research.

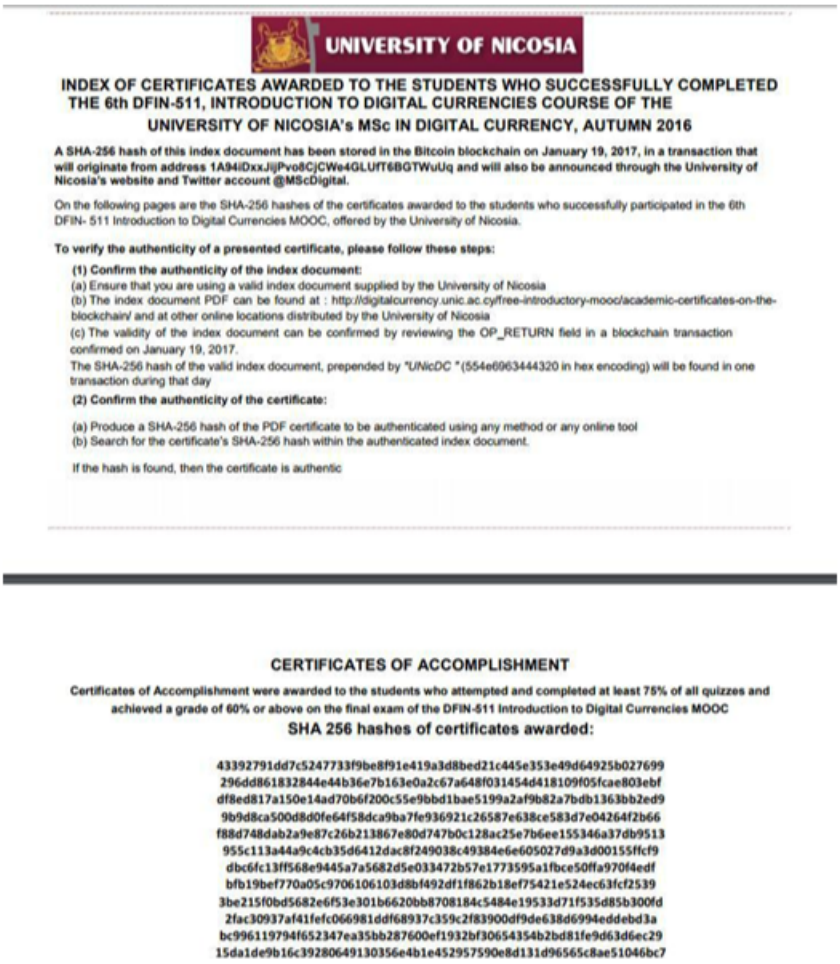
2.7.2 University of Nicosia

The University of Lefkosa (UNIC) has asked blockchain to organize "world principles" in its commitment to maximizing its instructive potential:

- Offer a scientific program that gives a certificate - science as a cash on the computer was blocked online as ASI - English (walked to begin learning in June 2014).
- Grant scientific certificates to Bitcoin Blockchain at the request program Stage (September 2014).

The course item is facilitated by the University of Nicosia (UNIC) and continues to advance through university systems in the world-wide educational community. The Centre-related disability chaining query positions itself as a world-class Center for untapped innovations that will coordinate, expand, and reinforce the region's curiosity-raising questioning in this progressive area.

University of Nicosia’s certificates are indexed on a web document as shown in Figure 7.



UNIVERSITY OF NICOSIA

INDEX OF CERTIFICATES AWARDED TO THE STUDENTS WHO SUCCESSFULLY COMPLETED THE 6th DFIN-511, INTRODUCTION TO DIGITAL CURRENCIES COURSE OF THE UNIVERSITY OF NICOSIA's MSc IN DIGITAL CURRENCY, AUTUMN 2016

A SHA-256 hash of this index document has been stored in the Bitcoin blockchain on January 19, 2017, in a transaction that will originate from address 1A94iDxxJijPvo8CjCWe4GLUfT6BGTWuUq and will also be announced through the University of Nicosia's website and Twitter account @MScDigital.

On the following pages are the SHA-256 hashes of the certificates awarded to the students who successfully participated in the 6th DFIN- 511 Introduction to Digital Currencies MOOC, offered by the University of Nicosia.

To verify the authenticity of a presented certificate, please follow these steps:

(1) Confirm the authenticity of the index document:

(a) Ensure that you are using a valid index document supplied by the University of Nicosia

(b) The index document PDF can be found at : http://digitalcurrency.unic.ac.cy/free-introductory-mooc/academic-certificates-on-the-blockchain/ and at other online locations distributed by the University of Nicosia

(c) The validity of the index document can be confirmed by reviewing the OP_RETURN field in a blockchain transaction confirmed on January 19, 2017.

The SHA-256 hash of the valid index document, prepended by *"UNicDC "* (554e6963444320 in hex encoding) will be found in one transaction during that day

(2) Confirm the authenticity of the certificate:

(a) Produce a SHA-256 hash of the PDF certificate to be authenticated using any method or any online tool

(b) Search for the certificate's SHA-256 hash within the authenticated index document.

If the hash is found, then the certificate is authentic

CERTIFICATES OF ACCOMPLISHMENT

Certificates of Accomplishment were awarded to the students who attempted and completed at least 75% of all quizzes and achieved a grade of 60% or above on the final exam of the DFIN-511 Introduction to Digital Currencies MOOC

SHA 256 hashes of certificates awarded:

43392791dd7c5247733f9be8f91e419a3d8bed21c445e353e49d64925b027699
296dd861832844e44b36e7b163e0a2c67a648f031454d418109f05fcae803ebf
df8ed817a150e14ad70b6f200c55e9bbd1bae5199a2af9b82a7bdb1363bb2ed9
9b9d8ca500d8d0fe64f58dca9ba7fe936921c26587e638ce583d7e04264f2b66
f88d748dab2a9e87c26b213867e80d747b0c128ac25e7b6ee155346a37db9513
955c113a44a9c4cb35d6412dac8f249038c49384e6e605027d9a3d00155ffcf9
dbc6fc13ff568e9445a7a5682d5e033472b57e1773595a1fbce50ffa970f4edf
bfb19bef770a05c9706106103d8bf492df1f862b18ef75421e524ec63fcf2539
3be215f0bd5682e6f53e301b6620bb8708184c5484e19533d71f535d85b300fd
2fac30937af41fefc066981ddf68937c359c2f83900df9de638d6994eddebd3a
bc996119794f652347ea35bb287600ef1932bf30654354b2bd81fe9d63d6ec29
15da1de9b16c39280649130356e4b1e452957590e8d131d96565c8ae51046bc7

Figure 7. University of Nicosia index of certificates

2.7.3 Bitcoin for Payment

Teachers allocate this early preference as critical benefits for their students and college:

- It was wise to accept online payments using a digital currency. This immediately showed that UNIC chose unused innovation and offers.
- The master's program has enabled him to draw the cohesion of a truly multi-national mummified relationship arising from the creation of a large number of nations. Foreign agreements are a rule related to the request of the so-called referral cases.

- Recovering the framework for issuing certificates and obtaining information will not fundamentally solve the regular problems for disputes. The capacity to create an installment framework without a mediator supplier increases the respect of both parties on the stock market. UNICEF offers a motivating power to pay for its target in Bitcoin, the installment portal, which it owns, and reduces it to 5% of all net fees. To help someone pay, and moreover to receive additional miles from a registration point to reach higher instructions: an outcast is allowed to be paid for the program, which is directed to ensure home availability.

2.8 Related Research

Since Blockchain is relatively a new technology in industry and academia, the number of applied cases and researches are slightly limited.

2.8.1 Blockcerts

Blockcerts (https://www.blockcerts.org) could be count as a significant example for related work. It is an open standard for Blockchain Credentials and supported by MIT's Media Lab and Learning Machine. Regardless this system also offers blockchain-enabled certificates, the blockcerts protocol is limited to verification of certificates. Blockcerts' certification flow is shown in Figure 8.

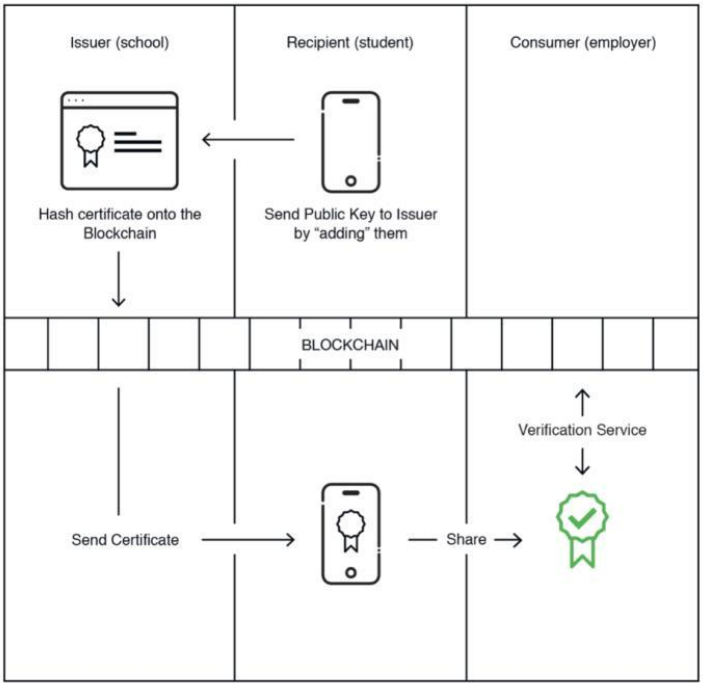


Figure 8. A sample process for verification of certificates in blockchain (Blockcerts, 2016)

2.8.2 Cardano

Greece's national research and education network (GRNET) also has work on a pilot project with the blockchain company IOHK to verify student diplomas on Cardano blockchain network (https://steemit.com/bitcoin/@steemi-news/cardano-s-first-use-case-certification-of-university-degrees-in-greece). This system is also only designed to verify graduation diplomas.

Chapter 3

IMPLEMENTATION

In this section, a sample implementation of authentication system of online student profiles is recommended as a proof of concept (PoC) work. PoC's scope is limited to necessary properties of simple authentication system of online student profiles on a blockchain.

First, to provide features for PoC, all requirements and assumptions are described together with user stories. Efforts have been made to minimize user stories and requirements and to keep the PoC at an applicable level of usability and security. Additional explanations for PoC, such as software diagrams, are also provided.

See the 3.2 for further implementation details.

3.1 User Stories and Features

3.1.1 Business Requirements

The high-level business goals of the products are:

- A blockchain platform will be used.
- Smart contracts will be programmable on the blockchain.

3.1.2 Functional Requirements

The application outlined in this thesis is limited to three types of businesses: users, organizations and guests. To define the various functional requirements that users have in practice, some user stories are written and the following Table 1 is shown. Also the functional requirements are shown by actors in Figure 9.

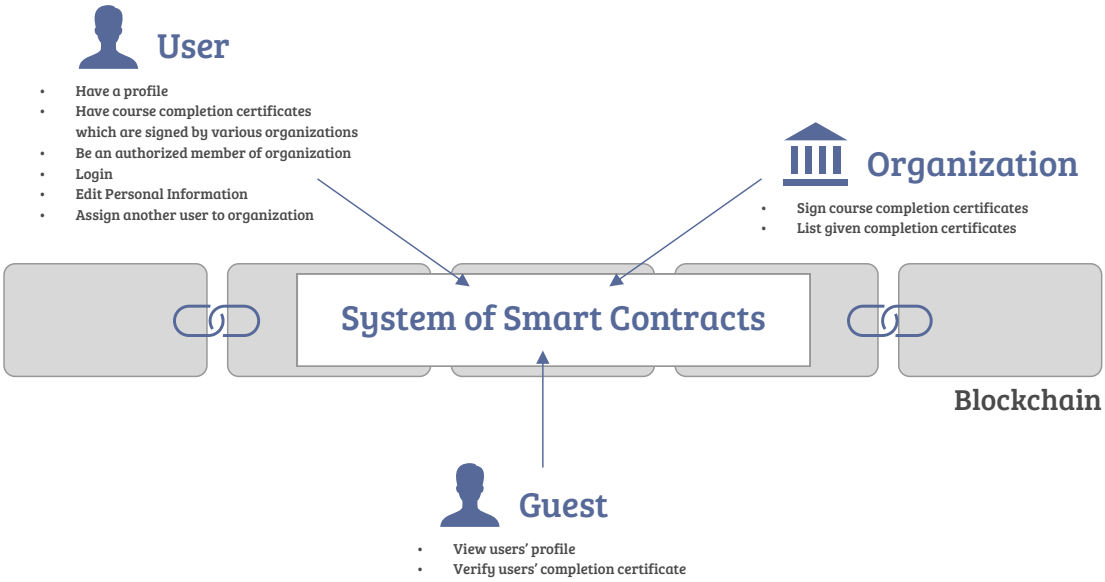


Figure 9. Overview of different actors and their interactions with the blockchain and system of smart contracts which exist on the blockchain

Table 1. User stories defining functional requirements and guiding development of authentication system PoC

As a…	I want/need to…	Traceability
User	Have a profile	1.1
	Have course completion certificates which are signed by various organizations	1.2
	Be an authorized member of organization	1.3
	Login	1.4
	Edit Personal Information	1.5
	Assign another user to organization	1.6
Organization	Sign course completion certificates	2.1
	List given completion certificates	2.2
Guest	View users' profile	3.1
	Verify users' completion certificate	3.2

Users are considered as accounts for users of the system. Each user can have a profile and sign the completion certificates, but they can't sign any certificates on their own. Organizations are considered virtual identities that can sign completion

certificates. There is no organization account on the system, but users can be selected as members of an organization.

3.2 Design of the PoC

In this section, the design of the PoC, which is based on the user stories is described. First of all, the smart contracts, which are the core of the PoC logic, is described. Thereafter, a proposal and and example for deployment on a blockchain is provided along with a clarification of the funcionality which that is required. Contract names and functions will be written underlined from now on to discriminate them.

3.2.1 Design Overview

In Figure 10, a high-level overview is provided of the Authentication System PoC. It goes from abstraction at the top level which is called “Software System Level”, to lower level of abstraction in the bottom, which is called “Contract Level”.

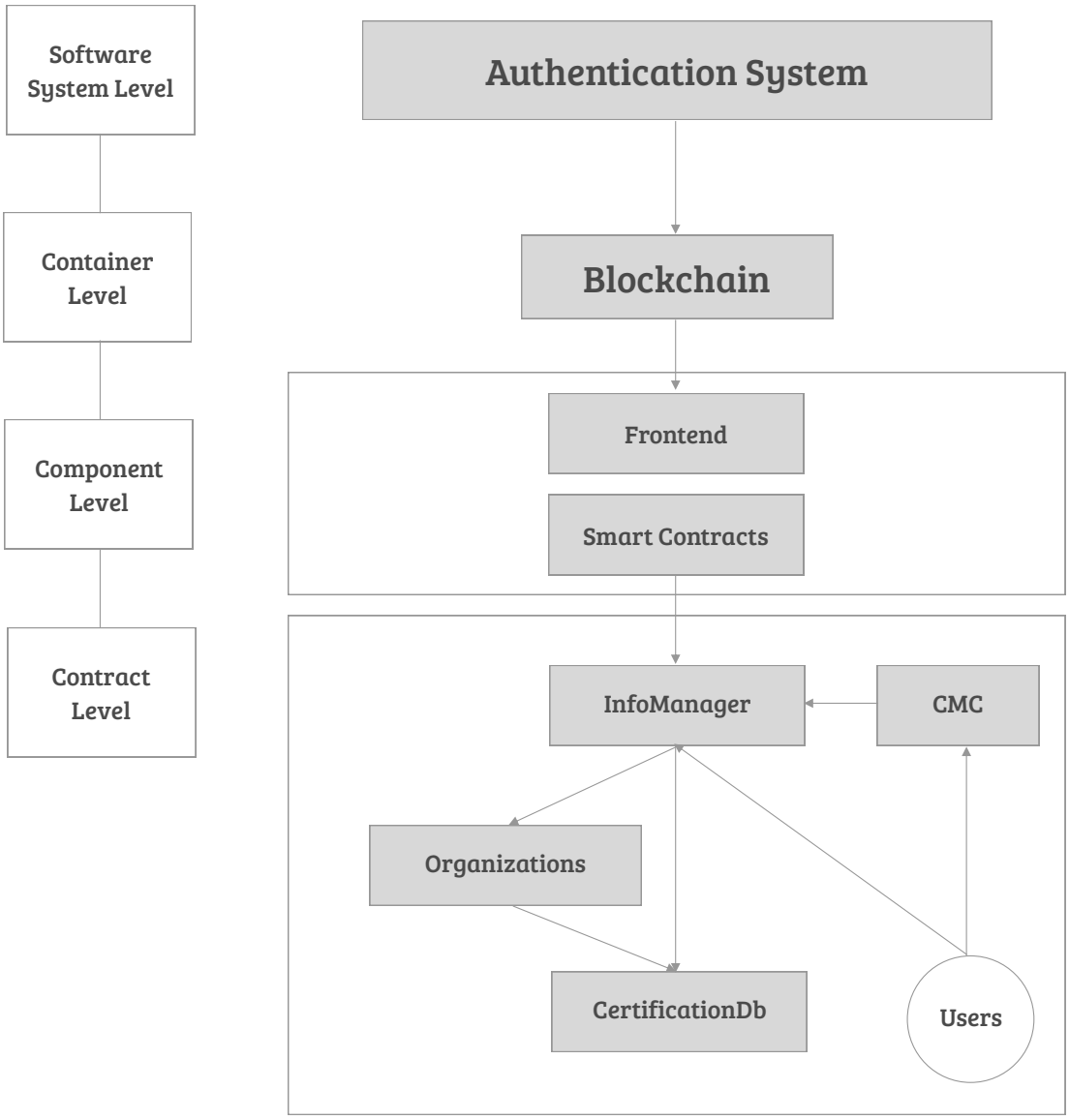


Figure 10. High-level system overview of the authentication system PoC. Visualisation technique is based on (Brown, 2016)

Blockchain is immutable due to its basic structure. For this reason, data such as adding a record at the end of a list that we are familiar with is done through different patterns. One of these patterns is the Contract-Managing-Contract (CMC) method. The CMC itself is a simple smart contract and keeps address information. In our design using CMC, we are able to add a completed course to a student's educational history as well as to define a new organization or organizational authority in the system.

In the design, the solidity codes for the InfoManager, Cmc, CertificationDb can be accessed with the file headings of the same name under appendices.

Solidity codes with the headings Organization and Student, which can be found under the appendices, include organization and user system methods.

3.2.2 Design and Development Tools

JavaScript language was used for both client-side and server-side development of the PoC. As a JavaScript blockchain development framework, Truffle also may be used to speed up development process (https://github.com/arvindkalra/express-box).

Ethereum was the choice of the platform for running smart contracts. In addition, the functional testing and fine tuning of the system was done using the online compiler which was provided by Ethereum foundation. The construction of smart contracts was done using Solidity language.

Web3 was the library used for integration between JavaScript and Ethereum.

3.2.3 System of Smart Contracts

The architecture proposed by the intelligent contracts system is based on the design principle in which different types of contracts perform different tasks. A model called “Five types of models” is used to classify such works and contracts (“Monax - solid description: five types of models, 2016”). However, all five models are not used in the PoC.

The Model distinguishes contracts as database, controller, contract management, application logic and service contracts. According to the model, the course finishing data will be stored in the database agreement. Each user's corresponding course completion certificate information is contained by a data structure called CertificationDb.

As a liaison management contract, a separate business name CMC will be designed. And all affiliate contracts are expected to be sourced from CMC interfaces.

Users and organizations will have application logic agreements to fulfill the business rules of the designed system.

To implement the application in a real-life scenario, one needs to build a blockchain. This setup requires that each node create a separate public and private key pair. Then, the developer initializes the original node, which holds the configuration information necessary for the blockchain to function properly.

The developer can define which private keys (validators) can be validated and connect to the blockchain. The authenticators are configured, the blockchain is started, and the transmissions can begin. Then, the developer publishes the contract to manage the contract, followed by other contracts. Thereafter, it saves other contracts to the contract management contract and sets permissions for users.

Since each saved contract has own address on the blockchain, these contracts can be called externally. Initiating a transaction to contract addresses is required to invoke any method defined in smart contracts. Therefore, an external system like a web service also could be designed and implemented. See 3.3 Running Steps of the PoC for details.

3.2.4 Data and Variables on the Blockchain

User and Organization data are expected to be stored in the blockchain. Because raw plain text data can cause a user to be identified, some of the details are masked as numeric identifiers in the blockchain. This will enable blockchain participants to see the course completion details of a particular person. However, if the specificity is reduced to prevent such users from being identified, the value at 0x4b39f9 will be “complete user x's course”. Thus, it is assumed that raw and plain text fields are stored in smart contracts.

3.3 Running Steps of the PoC

Genache and Truffle is used in development of this PoC. Development steps are listed:

- Installing node.js on the system.
- Installing Truffle and Ganache CLI globally with npm.
- Downloading arvindkalra/express-box truffle box.
- Creating the required files listed on the appendices.
- Starting ganache personalised blockchain development environment.
- Installing npm dependencies to the codebase.
- Running truffle compilation process.
- To deploy contracts for the first time, migration command of the truffle is needed to be used.
- Starting express http web server.

Detailed instructions can be found at express-box's GitHub account on the address https://github.com/arvindkalra/express-box.

Chapter 4

EVALUATION

In this chapter, the thesis which was presented in Chapter 3 will be evaluated using a descriptive evaluation method as proposed in Hevner et al., 2004.

4.1 Description of Evaluation Criteria

The IT artifact can be evaluated according to the criteria: "functionality, completeness, consistency, accuracy, performance, reliability, usability, fit with the organisation, and other relevant quality attributes." (Hevner et al., 2004). However, because the blockchain technology is still quite fresh, the scope of the thesis and the limits of the PoC, the artifact evaluation can't be done with all criterias (Hevner et al., 2004). These new methods should be used only when ther current methods are not effective, and the the new method is contemporary comparing to former ones. The Authentication System fits into this criteria, and so it will be evaluated using Informed Argument and Scenerio methods from descriptive evaluation theory.

Evaluation by Informed Argument is backed by an argument based on a knowledge base or relevant research.

Evaluation by a Scenerio is depending on construction of a well-defined specific use case.

4.2 Fulfilment of Evaluation Criteria

The Authentication System PoC fulfills the required functional criterias shown in Table 1. For the code details, the readers are provided with appendix providing a place where the whole source code is provided. Along with the functional criteria, to

cover non-functional aspects of PoC, additional requirements were defind. These are appraised in the argumentation based on the theory found in Chapter 2 in the thesis.

4.2.1 Potential Security and Privacy Exploits

The most crucial non-functional requirement on the PoC is the security of the users' data. The design and the description regarding this design's security is described at Section 3.2.4. However, the publicity of the courses completed are not covered by the solution. In theory, if the system consists of very few people, and the attacker knew who these people were, she would merge these information and match who owns which blockchain address. As a result, for example, such attacker may obtain additional course completion data. Contrarily, if there are huge numbers of users, it's a fact that this data is not valuable.

Another thing to consider is not the blockchain itself, but the steps upon logging on to the client. If the ip is tracable and can be binded to an account address by a third-party, then the privacy claims would be flawed. As a result, in addition to blockchain, the foundation surrounding the blockchain must be done with great care, considering not a large amount users are benefitting from Tor network.

Table 2. Evaluation of user story acceptance based on the authentication system PoC

As a…	Traceability	Motivation for fulfilment
User	1.1	Student definition in CertificationDb
	1.2	CourseCompletions array definition in Student definition of CertificationDb
	1.3	Blockchain's own user identity
	1.4	Blockchain's own user identity
	1.5	Student contract's editDetails method
	1.6	Organization contract's addUser method
Organization	2.1	Organization contract's addCertificate method
	2.2	Organization contract's listCertificates method
Guest	3.1	Student contract's getCertificate method

In this PoC, there are at least two layers of permissioning. In which the blockchain is a permissioned blockchain, and for smart contracts containing logic independent from the blockchain layer. Additionally, there are other steps of security one would have to go through to have access and permission on the blockchain. Because the implementation advises to use a blockchain, and as long as two thirds of the validators on the blockchain are charitible, the data of the events, such as prescription, purchase time and place can be considered safe and be stored immutably.

Additionally, explicit logging can also be build using the smart contracts, such as triggering a separate system to redundantly keep the records. The contracts are built with functional fashion, and also interact with a master, contract-managing contract. What this means is that any updates to contract system need to make a call to contract-managing contract. Therefore, any possible updates done to this system will not affect any application or other aspects communicating with blockchain, because the address of interface contract will remain the same.

4.3 Outcome

Considering all the functionality, abilities, completeness, security and privacy features, the artifact and the reasoning behind is would be considered a suitable for the usage of such an application for an Authentication System.

One of the reasons for this is that our work is fed from pure returns of the blockchain, in other words, providing a reliable, verifiable and permanent data chain electronically without the need for 3rd parties. Thanks to this structure, each party involved in the blockchain is able to verify the data independently from a central authority. Together with the high number of validators, the exchange of education information on the chain is easily achieved.

It can be mentioned that such a network of information, which is widespread and trustable, gives new opportunities to students who draw the path of learning. For example, some courses that are taken under a university, may require certain other courses to be taken before (prerequisites). While there is no such problem under the roof of the same institution, if you continue your education in a different faculty and if you are able to convince the educational institution, it starts the process of a complicated process.

For this reason, prerequisite courses or elective courses (or courses such as these) can't be exempted from the curriculum in different faculties which might lead to a situation where the course has to be repeated, it can't be taken from a desired educator or not to be taken at all. With the creation of the proposed system, these processes are rapidly transformable from physical documents to digital verification. In this way, even if the students cannot apply for a single diploma or certification program and cannot find a specialist in their respective faculty, they can reach the educational resource they want to specialize in a different university.

Chapter 5

CONCLUSION

This thesis establishes that the education ecosystem worldwide is becoming increasingly diversified and constantly evolving. The necessities of an authentication system suitable to said ecosystem are identified. Consequently, a novel approach is proposed: A decentralized and trusted information system that ensures the longevity, interoperability, verifiability of all course data, individuals' completion progress and assisting in design of their learning path with the aid of the new technology.

A system based on the blockchain concept is demonstrated to be appropriate, and a proof-of-concept implementation is proposed.

The proposed system enables complete data decentralization and securely verifiable consistency. The Ethereum blockchain platform and its toolchain are utilized to achieve peer to peer information storage and smart contract development.

The final proof-of-concept system was evaluated according to established design research criterion and requirements. Additionally, all research questions are addressed by the theory chapters of the thesis, as well as the design choices of the system.

Comparing to alternatives like Blockcerts, the proposed solution answers additional requirements by enabling interorganization information sharing in scope of indidivual profiles.

5.1 Generalisation and Extension Into Other Domains

The scope of this thesis is strictly limited to a specific solution. Regardless its initial purpose, this scope can be expanded with new requirements.

Since a decentralized data verification under user profiles solution is purposed, the work has the potential to be extended into any other domain has similar workflow.

5.2 Future Work

Blockchain is relatively a new technology in IT solutions. Many practices of today's blockchain will change and/or updated and some approaches will be reformed in the future. However, the blockchain community mostly focused on cryptocurrency needs, there are still issues lacks maturity.

In the context of this thesis, there could be additional user stories which could be extend work scope for further development. For example, introducing a functionality for linking prerequisite completions in spite of chaining an education path. Or creating a completely blockchain-based version of education tools, including learning management systems and student information systems, etc.

REFERENCES

Aglietti, A. (2017), Proof-Of-Knowledge: Same Blockchain, Different Story. https://tail.aqquadro.it/proof-of-knowledge-efc138f2a17c (4 Mart 2018).

Allen, I. E., Seaman, J. (2010), *Class Differences: Online Education in the United States*, Wellesley, MA.

Allen, C. (2016), The Path to Self-Sovereign Identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign identity.html (20 Şubat 2018)

Alonso G., Casati F., Kuno H., Machiraju V. (2004), *Web Services. In: Web Services. Data-Centric Systems and Applications.* Springer, Berlin, Heidelberg.

Au, S. (2017), Don't Forget What Self Sovereign Identity System Uport Doesn't Claim To Do, https://decentralize.today/dont-forget-what-self-sovereign-identity-system-uport-doesn-t-claim-to-do-1f43ca228575.

Beck, R., Czepluch, J., S.,Lollike, N., Malone, S. (2016). *Blockchain – The Gateway to Trust-Free Cryptographic Transactions*. In Research Papers from ECIS2016.

Byrne, W., I. (2017). What is the Blockchain? https://medium.com/badge-chain/what-is-Blockchain-5e4498f05c20

Camilleri, A. (2017). Outline of a trust and recognition structure for qualifications in Europe. https://doi.org/10.6084/m9.figshare.5372758.v1

Cheng, S., Daub, M., Domeyer, A., Lundqvist, M., (2016), Using Blockchain To Improve Data Management In The Public Sector, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-Blockchain-to-improve-data-management-in-the-public-sector

Christensen, Clayton M. (2003), *The Innovator's Solution: Creating and Sustaining Successful Growth*, Harvard Business Press.

Collins, M. (2002), *Ranking Algorithms for Name Entity Extraction: Boosting and the Voted Perceptron*, In Proceedings of ACL.

Cormier, D., Siemens, G. (2010). Through The Open Door: Open Courses As Research, Learning, And Engagement, DUCAUSE Review, *45*(4) 30-39.

EDUCAUSE Evolving Technologies Committee (2003), *Course Management Systems (CMS)*, http://www.educause.edu/ir/library/pdf/DEC0302.pdf

Fritz, J. (2011), *Classroom Walls That Talk: Using Online Course Activity Data Of Successful Students To Raise Selfawareness Of Underperforming Peers*, The Internet and Higher Education, *14*(2), 89–97.

Gibson, D., Ostashewski, N., Flintoff, K., Grant, S., Knight, E. (2015), *Digital Badges In Education*. Education and Information Technologies, *20*(2), 403-410.

Glance, D. (2013), The Teaching and Learning Foundations Of Moocs, *4*.

Greenberg, M. T. (1998), *Current and future challenges in school-based prevention: The researcher perspective.* Prevention Science

Gupta, V. (2017), *European Parliament Blockchain Presentation,* https://www.youtube.com/watch?v=fCYT9KWoldI

Hanson, R.T., Staples, M. (2017). *Distributed Ledgers, Scenarios For The Australian Economy Over The Coming Decades*, Canberra. Commonwealth Scientific and Industrial Research Organisation.

IBM (2017), *Blockchain Basics: Introduction To Distributed Ledgers*, https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html

Jagers, C. (2017), *Digital Identity And The Blockchain*, https://medium.com/learning-machine-blog/digital-identity-and-the Blockchain-10de0e7d7734

Januszewski, A., Molenda, M. (2013). *Educational Technology: A Definition with Commentary*. Routledge.

Keegan, D. (1995), *Distance Education Technology For The New Millennium:*

Compressed Video Teaching, ZIFF Papiere. Hagen, Germany: Institute for Research into Distance Education.

Lewis, A. (2017), *A Gentle Introduction To Self-Sovereign Identity*. https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity

Li, R. (2017), *Blockchain Based Multi-Signature Educational Certificate,* University of Birmingham. Unpublished paper.

Lilic, J. (2015), *uPort; A Glimpse into a Next Generation Self Sovereign Identity System*, https://www.linkedin.com/pulse/uport-glimpse-next-generation-self-sovereign-identity-john-lilic

Mamoria, M. (2017), *WTF Is The Blockchain? The Ultimate 3500-Word Guide In Plain English To Understand Blockchain*, https://hackernoon.com/wtf-is-the-Blockchain-1da89ba19348

Marvin, R. (2017). *Blockchain in 2017: The Year of Smart Contracts*, http://www.pcmag.com/article/350088/Blockchain-in-2017-the-year-of-smart-contracts

McKinsey (2016), *How Blockchains Could Change The World*, http://www.mckinsey.com/industries/high-tech/our-insights/how-Blockchains-could-change-the-world

Schmidt, J.P. (2015), *Certificates, Reputation, and the Blockchain*,

https://medium.com/mit-media-lab/certificates-reputation-and-the-blockchain-aee03622426f

Schmidt, J., P. (2017), *Credentials, Reputation, and the Blockchain*. http://er.educause.edu/articles/2017/4/credentials-reputation-and-the-Blockchain

Smolenski, N. (2016), *Identity and Digital Self-Sovereignty. A New Paradigm for Sovereignty on the High Seas*. Retrieved from: https://medium.com/learning-machine-blog/identity-and-digital-self-sovereignty-1f3faab7d9e3

Smolenski, N. (2017), *Blockchain Records for Refugees*, https://medium.com/learning-machine-blog/Blockchain-records-for-refugees-bd27ad6e6da1

Stiehl, R., Lewchuk, L. (2005), *The Assessment Primer: Creating A Flow Of Learning Evidence*, Corvallis, OR: The Learning Organization.

Tallent-Runnels, M. K., Thomas, J. A., Lan, W. Y., Cooper, S. , Ahern, T. C., Shaw, S. M., Liu, X. (2006). *Teaching Courses Online: A Review Of The Research*, Review of Educational Research, *76*(1), 93–135.

Teaster, P., Blieszner, R. (1999). Promises And Pitfalls Of The Interactive Television Approach To Teaching Adult Development And Aging, Educational Gerontology, *25*(8), 741-754.

Technavio (2017), Global Student Information System Market 2017-2021.

Thompson, S. (2017), *The Preservation Of Digital Signatures On The Blockchain*, The UBC iSchool Student Journal, *3*.

U.S. General Accounting Office (2002), Distance Education: Growth In Distance Education Programs And Implications For Federal Education Policy (Statement of Cornelia M. Ashby, Director, Education, Workforce, and Income Security Issues.

Using data to improve online courses (2011), *Distance Education Report*, http://www.magnapubs. com/newsletter/story/5718/

Watson, W. R., Lee, S., Reigeluth, C. M. (2007), *Learning Management Systems: An Overview And Roadmap Of The Systemic Application Of Computers To Education,* London.

Watson, W. R., Watson, S. L. (2007), *An Argument For Clarity: What Are Learning Management Systems, What Are They Not, And What Should They Become?* TechTrends, *51*(2), 28–34.

Western Cooperative for Electronic Telecommunications (WCET), UT TeleCampus, & Instructional Technology Council. (2009), *Best Practice Strategies To Promote Academic Integrity In Online Education, Version 2.0.* http://wcet. wiche.edu/wcet/docs/cigs/studentauthentication/BestPractices.pdf

Zhao, Y., Lei, J., Yan, B., Lai., C., Tan, S. (2005), *What Makes The Difference? A Practical Analysis Of Research On The Effectiveness Of Distance Education*, Teachers College Record, *107*(8), 1836–1884.

APPENDICES

Appendix A: Codebase

```
const contract = require('truffle-contract');
const Web3 = require('web3');

const metacoin_artifact =
require('../build/contracts/MetaCoin.json');
var MetaCoin = contract(metacoin_artifact);

module.exports = {
    init: function () {
        var self = this;

        // fallback - use your fallback strategy (local
node / hosted node + in-dapp id mgmt / fail)
        self.web3 = new Web3(new
Web3.providers.HttpProvider('http://localhost:8545'));
    },
    start: function (callback) {
        var self = this;

        // Bootstrap the MetaCoin abstraction for Use.

MetaCoin.setProvider(self.web3.currentProvider);

        // Get the initial account balance so it can be
displayed.
        self.web3.eth.getAccounts(function (err, accs) {
            if (err != null) {
                alert('There was an error fetching your
accounts.');
                return;
            }

            if (accs.length == 0) {
                alert('Couldn\'t get any accounts! Make
sure your Ethereum client is configured correctly.');
```

```
                return;
            }
            self.accounts = accs;
            self.account = self.accounts[2];

            callback(self.accounts);
        });
    },
    refreshBalance: function (account, callback) {
        var self = this;

        // Bootstrap the MetaCoin abstraction for Use.

MetaCoin.setProvider(self.web3.currentProvider);

        var meta;
        MetaCoin.deployed().then(function (instance) {
            meta = instance;
            return meta.getBalance.call(account, { from:
account });
        }).then(function (value) {
            callback(value.valueOf());
        }).catch(function (e) {
            console.log(e);
            callback('Error 404');
        });
    },
    sendCoin:  function  (amount,  sender,  receiver,
callback) {
        var self = this;

        // Bootstrap the MetaCoin abstraction for Use.

MetaCoin.setProvider(self.web3.currentProvider);

        var meta;
        MetaCoin.deployed().then(function (instance) {
            meta = instance;
```

```
            return  meta.sendCoin(receiver,  amount,  {
from: sender });
        }).then(function () {
            self.refreshBalance(sender,        function
(answer) {
                callback(answer);
            });
        }).catch(function (e) {
            console.log(e);
            callback('ERROR 404');
        });
    }
}
```

```
const express = require('express');
const app = express();
const port = 3000 || process.env.PORT;
const truffle_connect = require('./connection/app.js');
const bodyParser = require('body-parser');

// parse application/x-www-form-urlencoded
app.use(bodyParser.urlencoded({ extended: false }));

// parse application/json
app.use(bodyParser.json());

app.use('/', express.static('public_static'));

app.get('/getAccounts', (req, res) => {
    console.log('**** GET /getAccounts ****');
    truffle_connect.start(function (answer) {
        res.send(answer);
    })
});

app.post('/getBalance', (req, res) => {
```

```
    console.log('**** GET /getBalance ****');
    console.log(req.body);
    let currentAcount = req.body.account;

    truffle_connect.refreshBalance(currentAcount,
(answer) => {
        let account_balance = answer;
        truffle_connect.start(function (answer) {
            // get list of all accounts and send it along
with the response
            let all_accounts = answer;
            response = [account_balance, all_accounts]
            res.send(response);
        });
    });
});

app.post('/sendCoin', (req, res) => {
    console.log('**** GET /sendCoin ****');
    console.log(req.body);

    let amount = req.body.amount;
    let sender = req.body.sender;
    let receiver = req.body.receiver;

    truffle_connect.sendCoin(amount,  sender,  receiver,
(balance) => {
        res.send(balance);
    });
});

app.listen(port, () => {
    truffle_connect.init();

    console.log('Express Listening at http://localhost:'
+ port);
});
```

Cmc.sol

```
pragma solidity ^0.5.0;

import "./CmcEnabled.sol";
import "./Ownable.sol";

// The Contract managing contract.
contract Cmc is Ownable {
    // This is where we keep all the contracts.
    mapping(bytes32 => address) public contracts;

    // Add a new contract to Cmc. This will overwrite an
existing contract.
    function addContract(bytes32 name, address addr)
external onlyOwner {
        CmcEnabled cmce = CmcEnabled(addr);

        // Don't add the contract if this does not work.
        address payable this_ =
address(uint160(address(this)));

        cmce.setCmcAddress(this_);
        contracts[name] = addr;
    }

    function getContract(bytes32 name) external view
returns (address) {
        return contracts[name];
    }

    // Remove a contract from Cmc. We could also
selfdestruct if we want to.
    function removeContract(bytes32 name) external
onlyOwner returns (bool) {
        require(contracts[name] != address(0x0));

        CmcEnabled cmce = CmcEnabled(contracts[name]);
        cmce.remove();
```

```
        contracts[name] = address(0x0);
        return true;
    }

    function changeContractCmc(bytes32 name, address
payable newCmc) external onlyOwner {
        CmcEnabled cmce = CmcEnabled(contracts[name]);

        cmce.setCmcAddress(newCmc);
    }
}
```

CmcEnabled.sol

```
pragma solidity ^0.5.0;

import "./ContractProvider.sol";

// Base class for contracts that are used in a cmc system.
contract CmcEnabled {
    address payable public Cmc;

    modifier isCmcEnabled(bytes32 name) {
        require(msg.sender                              ==
ContractProvider(Cmc).contracts(name));
        _;
    }

    function() external {
       revert();
    }

    function setCmcAddress(address payable cmcAddr)
external {
```

```
        // Once the cmc address is set, don't allow it to
be set again, except by the
        // cmc contract itself.
        require(Cmc == address(0x0) || msg.sender == Cmc);

        Cmc = cmcAddr;
    }

    // Makes it so that Cmc is the only contract that may
kill it.
    function remove() external {
        require(msg.sender == Cmc);
        selfdestruct(Cmc);
    }
}
```

ContractProvider.sol

```
pragma solidity ^0.5.0;

// Interface for getting contracts from Cmc
interface ContractProvider {
    function  contracts(bytes32  name)  external  returns
(address addr);
}
```

InfoManager.sol

```
pragma solidity ^0.5.0;

import "./ContractProvider.sol";
import "./CmcEnabled.sol";
import "./PermissionsDb.sol";
import "./Organization.sol";
```

```
import "./Permissions.sol";
import "./Student.sol";
import "./Pharmacy.sol";

// The info manager
contract InfoManager is CmcEnabled {
    // We still want an owner.
    address owner;

    // Constructor
    constructor() public {
        owner = msg.sender;
    }

    // Attempt to complete a new course to a student
    function addCourseCompletion(address stdAddr, bytes32
courseCompletion) public payable returns (bool res) {
        if (courseCompletion == 0x0 || stdAddr ==
address(0x0)) {
            return false;
        }

        address organization =
ContractProvider(Cmc).contracts("organization");
        address permsdb =
ContractProvider(Cmc).contracts("permsdb");

        if (organization == address(0x0) || permsdb ==
address(0x0) || PermissionsDb(permsdb).perms(msg.sender)
< 1) {
            // If the user doesn't have the right to
complete, return false
            return false;
        }

        // Use the interface to call on the organization
contract. We pass drugHash and the student address along
as well.
```

```
        bool                    success                    =
Organization(organization).addStudent(msg.sender,
stdAddr, courseCompletion);

        // If the transaction failed, return the token to
the sender
        if (!success) {
            msg.sender.transfer(msg.value);
        }

        return success;
    }

    function    addStudent(address    stdAddr,    bytes32
courseCompletion) public payable returns (bool res) {
        uint8 requestCode = 2;

        if (stdAddr == address(0x0)) {
            return false;
        }

        address                organization                =
ContractProvider(Cmc).contracts("organization");
        address                    perms                   =
ContractProvider(Cmc).contracts("perms");

        if  (organization  ==  address(0x0)  ||  perms  ==
address(0x0) ||
            Permissions(perms).checkPerms(msg.sender) < 1
||
            Permissions(perms).checkConsent(msg.sender,
requestCode, stdAddr)) {
            // If  the  user  doesn't  have  the  right  to
complete return false
            // msg.sender.transfer(msg.value);
            return false;
        }
```

```
        // Use the interface to call on the organization
contract. We pass drugHash and the student address along
as well.
        bool                    success                 =
Organization(organization).addCourseCompletion(msg.sender
, stdAddr, courseCompletion);

        // If the transaction failed, return the token to
the sender
        if (!success) {
            msg.sender.transfer(msg.value);
        }

        return success;
    }

    function purchase(address stdAddr, bytes32 drugHash)
public payable returns (bool res) {
        if (drugHash == 0) {
            return false;
        }

        address                 pharmacy                =
ContractProvider(Cmc).contracts("pharmacy");
        address                 permsdb                 =
ContractProvider(Cmc).contracts("permissionsdb");

        if  (pharmacy  ==  address(0x0)  ||  permsdb  ==
address(0x0)  ||  PermissionsDb(permsdb).perms(msg.sender)
< 2) {
            // If the caller doesn't have permission to
complete a course, return false.
            return false;
        }

        // Use the interface to call on the organization
contract
```

```
        bool                    success                    =
Pharmacy(pharmacy).purchase(stdAddr, drugHash);

        // If the transaction succeeded, pass the token
back to the caller.
        if (success) {
            msg.sender.transfer(msg.value);
        }

        return success;
    }

    // Set the permissions for a given address.
    function setPermission(address addr, uint8 permLvl)
public returns (bool res) {
        address                 permsdb                =
ContractProvider(Cmc).contracts("permissionsdb");

        if (permsdb == address(0x0)) {
            return false;
        }

        uint8                   userPerm               =
PermissionsDb(permsdb).perms(addr);

        if (userPerm < 3) {
            return false;
        }

        return PermissionsDb(permsdb).setPermission(addr,
permLvl);
    }

    function setConsent(address addr, uint8 consentCode)
public returns (bool) {
        address                 student                =
ContractProvider(Cmc).contracts("student");
```

```
        if (student == address(0x0)) {
            return false;
        }

        return    Student(student).setConsent(msg.sender,
addr, consentCode);
    }
}
```

InfoManagerEnabled.sol

```
pragma solidity ^0.5.0;

import "./ContractProvider.sol";
import "./CmcEnabled.sol";

// Base class for contracts that only allow the infomanager
to call them.
// Note that it inherits from CmcEnabled
contract InfoManagerEnabled is CmcEnabled {
    // Makes it easier to check that infomanager is the
caller.
    function isInfoManager() public view returns (bool) {
        if (Cmc != address(0x0)) {
            address                  im                  =
ContractProvider(Cmc).contracts("infomanager");
            return msg.sender == im;
        }

        return false;
    }
}
```

Migrations.sol

```
pragma solidity ^0.5.0;

contract Migrations {
    address public owner;
    uint public last_completed_migration;

    modifier restricted() {
        if (msg.sender == owner) _;
    }

    constructor () public {
        owner = msg.sender;
    }

    function setCompleted(uint completed) public
restricted {
        last_completed_migration = completed;
    }

    function upgrade(address new_address) public
restricted {
        Migrations upgraded = Migrations(new_address);
        upgraded.setCompleted(last_completed_migration);
    }
}
```

Organization.sol

```
pragma solidity ^0.5.0;

import "./ContractProvider.sol";
import "./Cmc.sol";
import "./InfoManager.sol";
```

```
// An Organization
contract Organization is InfoManagerEnabled {
    // Register a student with address and (optionally)
courseCompletion
    function addStudent(address orgAddr, address stdAddr,
bytes32 courseCompletion) public payable returns (bool
res) {
        if (!isInfoManager()){
            return false;
        }

        address             certificationdb             =
ContractProvider(Cmc).contracts("certificationdb");
        if (certificationdb == address(0x0)) {
            // If the user sent a token, we should return
it if we can't complete.
            msg.sender.transfer(msg.value);

            return false;
        }

        // Use the interface to call on the certificationdb
contract. We pass msg.value along as well.
        bool                    success                 =
CertificationDb(certificationdb).addStudent(orgAddr,
stdAddr, courseCompletion);

        // If the courseCompletion failed, return the
Token to the caller.
        if (!success) {
            msg.sender.transfer(msg.value);
        }

        return success;
    }
```

```
    // complete a course, drughash for student with address
stdAddr
    function addCourseCompletion(address orgAddr, address
stdAddr, bytes32 courseCompletion) public payable returns
(bool res) {
        if (!isInfoManager()){
            return false;
        }

        address             certificationdb             =
ContractProvider(Cmc).contracts("certificationdb");

        if (certificationdb == address(0x0)) {
            // If the user sent a token, we should return
it if we can't complete.
            msg.sender.transfer(msg.value);
            return false;
        }

        // Use the interface to call on the studentdb
contract. We pass msg.value along as well.
        uint                    result                  =
CertificationDb(certificationdb).addCourseCompletion(orgA
ddr, stdAddr, courseCompletion);

        if (result == 0 || result == 1) {
            return false;
        }

        if (result == 2) {
            return true;
        }

        return false;
    }

    function   confirmCourseCompletion(address   stdAddr,
bytes32 drugHash) public payable returns (bool) {
```

```
        if (!isInfoManager()){
            return false;
        }

        address             certificationdb             =
ContractProvider(Cmc).contracts("certificationdb");
        if (certificationdb == address(0x0)) {
            msg.sender.transfer(msg.value);
            return false;
        }

        // Use the interface to call on the studentdb
contract. We pass msg.value along as well.
        return
CertificationDb(certificationdb).confirmCourseCompletion(
stdAddr, drugHash);
    }

    // Check if
    function    checkPrescripConsent(address    stdAddr,
bytes32 courseCompletions) internal pure returns (bool) {
    }

    function  isStudent(address  stdAddr)  public  returns
(bool) {
        if (!isInfoManager()){
            return false;
        }

        address             certificationdb             =
ContractProvider(Cmc).contracts("certificationdb");
        if (certificationdb == address(0x0)) {
            return false;
        }

        return
CertificationDb(certificationdb).isStudent(stdAddr);
    }
```

```
}
```

Ownable.sol

```
pragma solidity ^0.5.0;

// taken from OpenZeppelin
//          https://github.com/OpenZeppelin/openzeppelin-
solidity/blob/master/contracts/ownership/Ownable.sol

/**
 * @title Ownable
 * @dev The Ownable contract has an owner address, and
provides basic authorization control
 * functions, this simplifies the implementation of "user
permissions".
 */
contract Ownable {
    address private _owner;

    event       OwnershipTransferred(address       indexed
previousOwner, address indexed newOwner);

    /**
     * @dev The Ownable constructor sets the original
`owner` of the contract to the sender
     * account.
     */
    constructor () internal {
        _owner = msg.sender;
        emit OwnershipTransferred(address(0), _owner);
    }

    /**
```

```
     * @return the address of the owner.
     */
    function owner() public view returns (address) {
        return _owner;
    }

    /**
     * @dev Throws if called by any account other than the
owner.
     */
    modifier onlyOwner() {
        require(isOwner(), "Only owner can be call this
method.");
        _;
    }

    /**
     * @return true if `msg.sender` is the owner of the
contract.
     */
    function isOwner() public view returns (bool) {
        return msg.sender == _owner;
    }

    /**
     * @dev Allows the current owner to relinquish control
of the contract.
     * @notice Renouncing to ownership will leave the
contract without an owner.
     * It will not be possible to call the functions with
the `onlyOwner`
     * modifier anymore.
     */
    function renounceOwnership() public onlyOwner {
        emit OwnershipTransferred(_owner, address(0));
        _owner = address(0);
    }
```

```
    /**
     * @dev Allows the current owner to transfer control
of the contract to a newOwner.
     * @param newOwner The address to transfer ownership
to.
     */
    function transferOwnership(address newOwner) public
onlyOwner {
        _transferOwnership(newOwner);
    }

    /**
     * @dev Transfers control of the contract to a
newOwner.
     * @param newOwner The address to transfer ownership
to.
     */
    function _transferOwnership(address newOwner)
internal {
        require(newOwner != address(0x0), "New owner is
not set");
        emit OwnershipTransferred(_owner, newOwner);
        _owner = newOwner;
    }
}
```

Permissions.sol

```
pragma solidity ^0.5.0;

import "./ContractProvider.sol";
import "./InfoManagerEnabled.sol";
import "./PermissionsDb.sol";

// Permissions
contract Permissions is InfoManagerEnabled {
```

```
    // Set the permissions of an account.
    function setPermission(address addr, uint8 perm)
public returns (bool res) {
        if (!isInfoManager()) {
            return false;
        }

        address                permdb                =
ContractProvider(Cmc).contracts("permsdb");

        if (permdb == address(0x0)) {
            return false;
        }

        return  PermissionsDb(permdb).setPermission(addr,
perm);
    }

    function checkPerms(address addr) public pure returns
(uint) {
    }

    function    checkConsent(address    orgAddr,    uint8
consentCode, address stdAddr) public pure returns (bool)
{
    }
}
```

PermissionsDb.sol

```
pragma solidity ^0.5.0;

import "./ContractProvider.sol";
import "./CmcEnabled.sol";
```

```
// Permissions database
contract PermissionsDb is CmcEnabled {
    struct consentedStudentCourseCompletionTuple {
        address organization;
        bytes32 courseCompletion;
    }

    struct consentStudentCode {
        address orgOrPharm;
        uint8 consentCode;
    }

    mapping (address => uint8) public perms;
    mapping (address => consentStudentCode) public
studentOrganizationConsent;
    mapping (address => consentedStudentCourseCompletionTuple) public
prescripStudentConsent;

    // Set the permissions of an account.
    // Permissions:
    // 0 - student permissions, e.g. only allowed to read
info related to one's own address
    // 1 - Pharmacy permissions, e.g. allowed to read info
about student who shared it's address
    // 2 - organization permissions, allowed to add
students, add course completions and read info about
students
    function setPermission(address addr, uint8 perm)
public returns (bool res) {
        if (Cmc != address(0x0)) {
            address permC =
ContractProvider(Cmc).contracts("perms");

            if (msg.sender == permC) {
                perms[addr] = perm;
```

```
                return true;
            }
        }

        return false;
    }

    // Allow students to consent to other users to perfom
actions on their behalf such as adding course completions
    // Permissions:
    // 0 - no permission
    // 1 - addr, being a pharmacy, can sell prescribed
course completion to sender
    // 2 - addr, being a organization, can prescribe course
completion for sender
    // 3 - addr, being a organization, can add sender as
student with a course completion
    function    setConsent(address    stdAddr,    address
orgOrPharmAddr, uint8 consentCode) public returns (bool
res) {
        if (Cmc != address(0x0)) {
            address              studentC              =
ContractProvider(Cmc).contracts("student");

            consentStudentCode     memory     cons     =
consentStudentCode(orgOrPharmAddr, consentCode);

            if (consentCode < 4 && msg.sender == studentC)
{
                studentOrganizationConsent[stdAddr]     =
cons;

                return true;
            }
        }

        return false;
    }
```

```
    function setPrescripConsent(address stdAddr, address
orgAddr, bytes32 courseCompletion) public returns (bool
res) {
        if (Cmc != address(0x0)) {
            address              studentC             =
ContractProvider(Cmc).contracts("student");

            consentedStudentCourseCompletionTuple  memory
consPP  =  consentedStudentCourseCompletionTuple(orgAddr,
courseCompletion);

            if (msg.sender == studentC) {
                prescripStudentConsent[stdAddr] = consPP;

                return true;
            }
        }

        return false;
    }
}
```

Student.sol

```
pragma solidity ^0.5.0;

import "./ContractProvider.sol";
import "./PermissionsDb.sol";
import "./InfoManagerEnabled.sol";

// students
contract Student is InfoManagerEnabled {
    // Consent levels:
```

```
    // 0 - no permissions
    // 1 - addr, being a pharmacy, can sell prescribed
course completion to sender
    // 2 - addr, being a organization, can prescribe course
completion for sender
    // 3 - addr, being a organization, can add sender as
student with a courseCompletion
    // Set level of consent for a specific address
    function setConsent(address stdAddr, address addr,
uint8 consentCode) public returns (bool success) {
        if (!isInfoManager()){
            return false;
        }

        address             permissionsdb             =
ContractProvider(Cmc).contracts("permissionsdb");

        if (permissionsdb == address(0x0)) {
            // If the user sent a token, we should return
it if we can't complete.
            return false;
        }

        // Use the permissionsdb-interface to call on the
permissionsdb contract to set consent level
        success                                         =
PermissionsDb(permissionsdb).setConsent(stdAddr,    addr,
consentCode);
        return success;
    }

    // set courseCompletion consent
    function setPrescripConsent(address stdAddr, address
orgAddr, bytes32 courseCompletion) public returns (bool
res) {
        if (!isInfoManager()){
            return false;
        }
```

```
        address              permissionsdb              =
ContractProvider(Cmc).contracts("permissionsdb");
        if (permissionsdb == address(0x0)) {
            // Can't set consent.
            return false;
        }

        // Use the permissionsdb-interface to call on the
permissionsdb contract to set consent level
        res                                            =
PermissionsDb(permissionsdb).setPrescripConsent(stdAddr,
orgAddr, courseCompletion);

        return res;
    }

    function _getNumOfCourseCompletions(address stdAddr)
internal returns (uint256) {
        if (Cmc != address(0x0)) {
            address           certificationdb          =
ContractProvider(Cmc).contracts("certificationdb");

            if (certificationdb != address(0x0)) {
                CertificationDb           pat          =
CertificationDb(certificationdb);
                uint256               len              =
pat.getNumOfCourseCompletions(stdAddr);

                return len;
            }
        }
    }

    function getCourseCompletions() pure public {
    }
}
```

CertificationDb.sol

```
pragma solidity ^0.5.0;

import "./ContractProvider.sol";
import "./CmcEnabled.sol";

// The certification database
contract CertificationDb is CmcEnabled {
    // List element
    struct Student {
        address prev;
        address next;
        // Data
        bytes32[]   courseCompletions;   //   Array   of
courseCompletions;
        address[] responsible; // Array of responsible
person for corresponding course completion
        bool init;
    }

    uint public size;
    address public tail;
    address public head;
    mapping (address => Student) public studentList;
    //   mapping   (address   =>   bytes32[])   public
courseCompletions;

    // Add a new student with a course completion. This
will overwrite an existing course completion. 'internal'
modifier means
    // it has to be called by an implementing class.
    function addStudent(address respAddr, address stdAddr,
bytes32 courseCompletion) public returns (bool) {
        if (Cmc != address(0x0)) {
            address             organization          =
ContractProvider(Cmc).contracts("organization");
```

```
            if    (msg.sender    ==    organization    &&
studentList[stdAddr].init == false) {
                bytes32[] memory presc = new bytes32[](1);
                presc[0] = courseCompletion;

                address[] memory resp = new address[](1);
                resp[0] = respAddr;

                Student memory pat = Student(address(0x0),
address(0x0), presc, resp, true);
                studentList[stdAddr] = pat;

                // Two cases - empty or not.
                if (size == 0) {
                    tail = stdAddr;
                    head = stdAddr;
                }
                else {
                    studentList[head].next = stdAddr;
                    studentList[stdAddr].prev = head;
                    head = stdAddr;
                }

                size++;
                return studentList[stdAddr].init;
            }
        }

        return false;
    }

    function  addCourseCompletion(address  resp,  address
stdAddr,  bytes32  courseCompletion)  public  returns  (uint
result) {
        if (studentList[stdAddr].init == false) {
            // return code 0 means student not found
            return 0;
```

```
        }

        if (courseCompletion == 0) {
            // return code 1 means no courseCompletion
given
            return 1;
        }

        // return code 2 means courseCompletion added to
student

studentList[stdAddr].courseCompletions.push(courseComplet
ion);
        studentList[stdAddr].responsible.push(resp);

        return 2;
    }

    function _getCourseCompletionByIndex(address stdAddr,
uint8 index) public returns (bytes32) {
        if (Cmc != address(0x0)) {
            address             organization             =
ContractProvider(Cmc).contracts("organization");
            address               student                =
ContractProvider(Cmc).contracts("student");

            if (msg.sender == organization || msg.sender
== student) {
                if (studentList[stdAddr].init == false) {
                    // student not found
                    return 0x0;
                }

                return
studentList[stdAddr].courseCompletions[index];
            }
        }
    }
```

```
    function  getNumOfCourseCompletions(address  stdAddr)
public returns (uint256) {
        if (Cmc != address(0x0)) {
            address             organization             =
ContractProvider(Cmc).contracts("organization");
            address               student                =
ContractProvider(Cmc).contracts("student");

            if (msg.sender == organization || msg.sender
== student) {
                if (studentList[stdAddr].init == false) {
                    // student not found
                    return 0;
                }

                return
studentList[stdAddr].courseCompletions.length;
            }
        }
    }

    // requires the caller to know the hash of the
courseCompletion, confirms whether courseCompletion exists
or not
    function   confirmCourseCompletion(address   stdAddr,
bytes32 courseCompletion) public returns (bool) {
        if (Cmc != address(0x0)) {
            // Ensure caller is organization or pharmacy
            address             organization             =
ContractProvider(Cmc).contracts("organization");
            address               pharmacy               =
ContractProvider(Cmc).contracts("pharmacy");
            address               student                =
ContractProvider(Cmc).contracts("student");

            if (msg.sender == organization || msg.sender
== pharmacy) { // Ensure sender is organization or pharmacy
```

```
                if (studentList[stdAddr].init == false ||
courseCompletion == 0) {
                    return false;
                }

                for       (uint       i       =       0;
i<studentList[stdAddr].courseCompletions.length; i++) {

if(studentList[stdAddr].courseCompletions[i] != 0) {
                        return true;
                    }
                }
            }
            else if (msg.sender == student || msg.sender
== organization) { // If sender is neither organization
nor pharmacy, check if sender is student
                if (studentList[stdAddr].init == false ||
courseCompletion == 0) { // only allow student to confirm
                    return    false;    //    proprietary
courseCompletions
                }

                for    (uint    i    =    0;    i    <
studentList[stdAddr].courseCompletions.length; i++) {

if(studentList[stdAddr].courseCompletions[i] != 0 && i <
1000) { // Check if i:th
                        return true; // courseCompletion
is the requested one.
                    } // Cap at 1000 if list has length >
1000
                }
            }
        }

        return false;
    }
```

```
    function isStudent(address stdAddr) public view
returns (bool) {
        if (studentList[stdAddr].init == true) {
            return true;
        }

        return false;
    }
}
```

Appendix B: Originality Report

Turnitin Originality Report

Thesis_V06 by Eser Ozvataf

From Eser_Ozvataf (SCHOOL OF COMPUTING AND TECHNOLOGY)

- Processed on 21-Jan-2019 09:59 +03
- ID: 1066525554
- Word Count: 17011

Similarity Index
13%
Similarity by Source

Internet Sources:
11%
Publications:
3%
Student Papers:
9%

sources:

1 1% match (Internet from 24-Mar-2012)
http://learningoutcomesassessment.org/documents/OnlineEd.pdf

2 1% match (Internet from 11-Jan-2018)
http://www.pedocs.de/volltexte/2018/15013/pdf/Grech_Camilleri_2017_Blockchain_in_Education.pdf

3 1% match (Internet from 05-Oct-2018)
https://link.springer.com/article/10.1186/s40561-017-0050-x

4 1% match (student papers from 11-Sep-2017)
Submitted to Sim University on 2017-09-11

5 1% match (student papers from 30-Aug-2015)
Class: SCHOOL OF COMPUTING AND TECHNOLOGY
Assignment:
Paper ID: 564772539