https://doi.org/10.22364/atee.2019.itre.13

BLOCKCHAIN ARHITECTURE IN SMART PEDAGOGY

Andis Āriņš
University of Latvia, Latvia

ABSTRACT

Blockchain architecture in Smart Pedagogy offers valuable social propositions like trust, identity, transparency, immutability, smart contracts and disintermediation. There are multiple practices how to record learners' achievements and present learning transcripts where the most common practices are university issued diplomas and vendor issued certificates. There are social networks which allow users to publish their learning achievements for possible stakeholders; however, the common problem is to verify if published diplomas and certificates are valid.

This study experiments with lifelong learning transcript called knowledge passport in blockchain architecture. The proposed scenario allows learners to publish evidence of their learning achievements in desired formats connected with blockchain network for instant authenticity verification. The experimental network consists of three nodes where one is located in Latvia, the second – in the USA, and the third – in Asia. Based on the proposed implementation, such approach much better validates learning evidence, eliminates knowledge passport fraud and reduces organizational workload overhead for stakeholders involved in verification of documents certifying a person's knowledge.

Keywords: Blockchain architecture, modern education, Smart Pedagogy.

Introduction

Smart Pedagogy promotes synergy between pedagogy and technology in the context of modern education. Computing and digital developments has brought proposed learning strategies for promoting learning in technologically enriched environments. There are studies on smart education, even developments of smart education systems that improve learning experience and strives for extension of learning resource availability anywhere, anytime in an individually prepared manner. One of the Smart Pedagogy higher-level domains are aspects that need to be considered in pedagogical processes – attitude, motivation, knowledge, diversity, assessment (Daniela & Lytras, Learning Strategies and Constructionism in Modern Education Settings, 2018). This study proposes blockchain architecture as a decentralized database for storing learners' assessment results as lifelong learning transcript called knowledge passport. There are two main benefits in blockchain-based learning achievement design – first, instant authenticity verification if published diplomas or certificates are valid, second – adaptive learning customization for an individual learner based on previous assessment results.

Blockchain technology in one of its first proposals was introduced by W. Stuart Haber and Scott Stornetta in 1991 as computationally practical solution for timestamping digital documents, so that they could not be backdated or tampered with (Haber & Stornetta, 1991). Their initial work for time stamping a digital document relied on a central authority that had to record the date and time a certain document was created and store a copy of it. However, there was a problem of trust where authors acknowledged that nothing in this scheme prevents the time-stamping service from colluding with a client. As their original mission seemed impossible, they attempted to disprove the possibility of creating an immutable ledger but found an architecture that would not require a trusted central authority, so Stornetta and Haber succeeded in creating a distributed immutable ledger.

In 2004, a computer scientist Hal Finney introduced a system called RPoW, Reusable Proof of Work (Finney, 2004), Its main idea proposes a prototype for digital cash. RPoW solved a well-known double-spending problem by keeping the ownership of tokens registered on a trusted server where users via internet could verify token correctness and integrity in real time. RPoW is an important milestone in the history of cryptocurrencies.

In 2008, a paper for Bitcoin proposal was published – so far the most popular blockchain-based innovation called the first electronic cash system or digital currency (Nakamoto, 2008). Bitcoin is based on RPoW initial work, and it works as a decentralized peer-to-peer protocol for tracking and verifying transactions. Satoshi Nakamoto, the name under which Bitcoin article was published, is a pseudonym, and the real author or groups of authors are still unknown. It is interesting that Hal Finney participated as a receiver in the very first bitcoin transaction where he received 50 blocks from Satoshi Nakamoto, and so far he is the only one who has received bitcoin blocks from Satoshi Nakamoto (Bitcoin Transactions, 2019). Hal Finney has denied being Satoshi Nakamoto himself.

Digital currencies are only one of the cases when blockchain architecture is used. Blockchain is an incorruptible digital ledger of economic transactions that can be prepared to store not just digital currency transactions but virtually any valuable data stored in decentralized manner. If first blockchain developments were oriented to cryptocurrency, later developments focus also on smart contracts, and multi-field applications like healthcare, government services, science, culture and education. There are common blockchain implementation features shared by digital currencies which can be used also for storing other valuable data within environment where there is no central server or certification authority. Possible internet-based peer-to-peer network connections and digital signatures sign/encrypt transactions need to guarantee:

1) participant-consensus validated transactions;
2) transactions irreversibility where it is impossible to cancel a transaction;
3) counterfeiting where it is impossible to print digital money;
4) double-spending where it is impossible to spend the same value multiple times.

There is a published review that compares consensus protocols for blockchain architecture with respect to their fault models and resilience against attacks. The protocol comparison covers Hyperledger Fabric, Tendermint, Symbiont, R3 Corda, Iroha, Kadena, Chain, Quorum, MultiChain, Sawtooth Lake, Ripple, Stellar, and IOTA (Cachin & Vukolic, 2017). Online centralized single authority systems, blockchain architecture confirm data validity based on consensus protocol that in this research is selected to be Quorum for majority of stakeholders to control data provisioning and sequence.

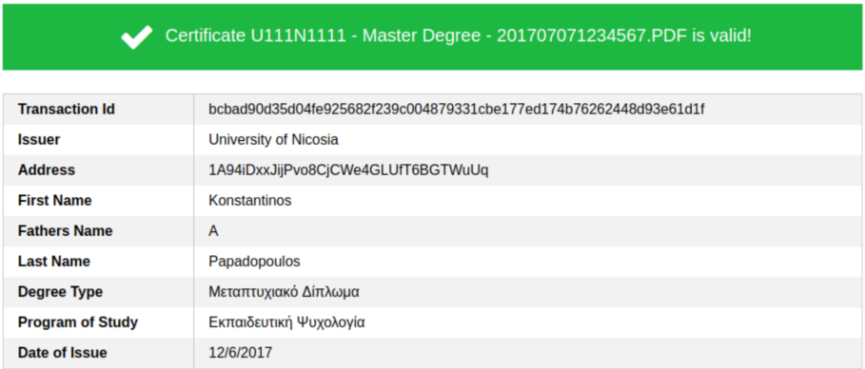
Historically education systems use certificates, diplomas, transcripts, learning records or any other type of assessment evidence documents mostly in paper format to confirm learning and its results. Such learning evidence documents in real life follow both academic (where final awards may contain degrees) or specific skills-oriented commercial training where final awards may contain specific titles like a certified professional. Learning evidence documents include important data blocks like the issuer, date of issue, validity, signing person, learner's name/surname and qualification degree or title. There are no common standards for learning evidence documents, so each academic or commercial learning organization can design its own document version. It is possible to implement and use some security mechanisms as holograms (in paper documents they are rarely used because of more complex printing and additional costs). In comparison, paper money has much better anti-fraud mechanisms. From third party perspective, it is challenging to verify such learning evidence documents, as it requires individual efforts to identify and contact the issuer to confirm validity of learning evidence document. University diploma validity research (Contreras & Gollin, 2010) studies fake diploma problem. In modern education systems, digitally signed certificates replace paper learning evidence documents. For the learner, it is an advantage but for the issuer such solutions rise responsibility to secure the database and the signing key. In addition, such issuers might consider storing publicly accessible database for verification purposes (MikroTik, 2019) as digital learning certificates not only expire but also the issuer can revoke them.

This study supplements the existing blockchain development in modern education and experiments with a dedicated blockchain network connected via internet protocol with 3 blockchain nodes based in three different continents. The main idea of this study is to experiment with learners' assessment results as a lifelong learning transcript called knowledge passport in secure, independent, quorum supported blockchain architecture. Although there are several proposals for digital proof of education certificates like unsecure simple PDF certificates, digitally signed PDF certificates or even digital currency-based (Bitcoin, Ethereum) proposals, none of them is accepted as general practice for presenting digital proof of learning evidence. This study is different from previously digital currency-based proposals, as it is using different, independent architecture controlled by education stakeholders with no need to pay settlements to digital currency miners for block confirmation. Each of blockchain architecture implementation domains has its own specifics that requires research and opportunities for innovators. Available blockchain-based ideas and appropriate studies for education domain are reviewed in the following section. The experimental setup description follows in the third section of this study. Experimentation results are presented in the fourth chapter of this paper, and the conclusion and future research proposals close this study.

Related research and developments

As of June 2019, there are dozens of universities offering studies of blockchains, cryptocurrencies, distributed consensus, smart contracts and applications. For example, University of California At Berkeley, Stanford University, Massachusetts Institute of Technology, IT University of Copenhagen and University of Nicosia – Cyprus offering MSc Degree in Digital Currency (UNIC, 2019). Students of University of Nicosia who successfully qualify will receive their academic certificates whose authenticity can be verified through the Bitcoin blockchain as presented in Fig. 1 (Nicosia, 2019).

Since July 2017, as part of its ongoing innovation around blockchain, the SAP innovation Center Network have introduced TrueRec - a secure and trusted digital wallet for storing professional and academic credentials powered by blockchain. These credentials could include anything from IDs, such as passport, driver's license, or voter ID, to education credentials like university degrees and employment certificates. TrueRec is powered by Ethereum, an open-source, public, blockchain-based distributed computing platform that features smart contract (scripting) functionality that facilitates online contractual agreements (SAP News Center, 2019).

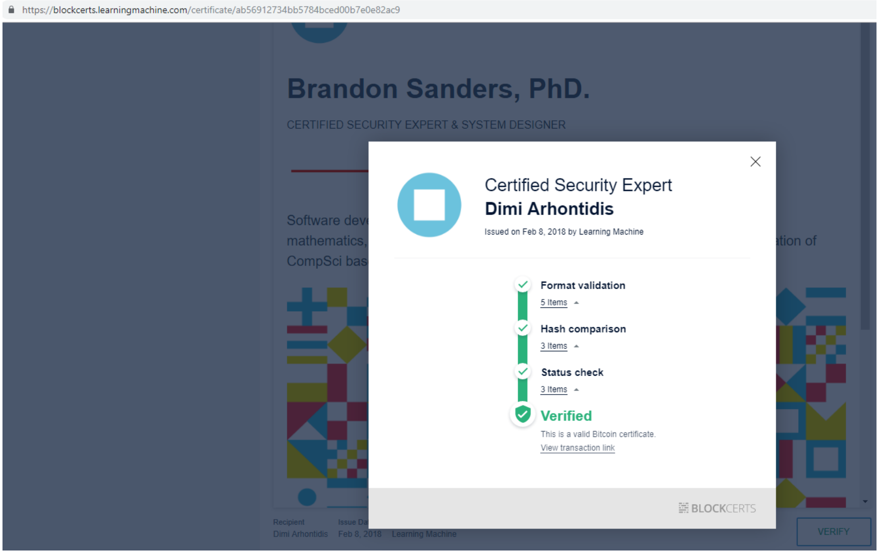


Certificate U111N1111 - Master Degree - 201707071234567.PDF is valid!

Transaction Id	bcbad90d35d04fe925682f239c004879331cbe177ed174b76262448d93e61d1f
Issuer	University of Nicosia
Address	1A94iDxxJijPvo8CjCWe4GLUfT6BGTWuUq
First Name	Konstantinos
Fathers Name	A
Last Name	Papadopoulos
Degree Type	Μεταπτυχιακό Δίπλωμα
Program of Study	Εκπαιδευτική Ψυχολογία
Date of Issue	12/6/2017

Figure 1. Nicosia MSc academic degree certificate verification

Since October 2016, Blockcerts proposal for open standard for creating, issuing, viewing, and verifying blockchain-based certificates contributes to the prototype developed by MIT Media Lab and Learning Machine initiative group. Blockcerts use Bitcoin blockchain as the provider of trust, and credentials are tamper-resistant and verifiable. Blockcerts can be used in the context of academic, professional, and workforce credentialing. At its core, Blockcerts is open code software (Blockcerts, 2019). Blockcerts relies on Bitcoin complexity and immutability as important and careful consideration for long-term effects. Sample Blockcert digital certificate verification is presented in Fig. 2 (Learning Machine, 2019).



https://blockcerts.learningmachine.com/certificate/ab56912734bb5784bced00b7e0e82ac9

Brandon Sanders, PhD.

CERTIFIED SECURITY EXPERT & SYSTEM DESIGNER

Certified Security Expert
Dimi Arhontidis
Issued on Feb 8, 2018 by Learning Machine

✓ **Format validation**
5 Items

✓ **Hash comparison**
3 Items

✓ **Status check**
3 Items

✓ **Verified**
This is a valid Bitcoin certificate.
View transaction link

Figure 2. Blockcert digital certificate verification

Among recent studies focusing on blockchain, there is a notable initiative by Gräther et al. proposing Lifelong Learning Passport solution for education domain. In Gräthers study first, author describes the conceptual system overview and presents in detail the platform implementation including management of certification authorities and certificates, smart contracts, as well as services for certifiers, learners and third parties, such as employers. Finally, author describes use-cases and first evaluation results gathered from end user tests with certifiers (Gräther, et al., 2018). Gräther platform is based on Ethereum contracts and is limited to OpenZeppelin approved smart contract templates

Blockchain featuring Smart Pedagogy

The core idea of smart pedagogy as technology-enhanced learning promotes meaningful usage of state-of-the-art technologies in transforming learning environments. Smart pedagogy can support educators in finding the answers on how to support learning in the transformed education process, how to incorporate technologies into learning to support the development of metacognition, how to support knowledge building, how to support the development of digital competences (Daniela, 2019). Novelty is not the only common characteristic shared by blockchain and smart pedagogy. This study proposes blockchain architecture as technology-enhanced learning advancement for the following benefits:

1) Lifelong learning transcript called the knowledge passport. There might be doubts because of privacy and other reasons regarding who and in what detail should be able to observe learners' achievements and results. Most often a learner would share his/her final learning result evidence document with third parties. However, it can be beneficial both for the learner and educator to zoom in the learner's assessment results on a subject or even topic level. Depending on the learners and educator's agreement, technically the knowledge passport could contain results of all assessments ever taken by the learner. Blockchain architecture serves as a decentralized platform for storing hashed references to recorded learning results as stored in a distributed secure network that does not allow data tampering. For example, if the learner demonstrated poor results on a topic and later repeated the test with better results, the knowledge passport would store both the old and the new result. Having access to a trusted learner's lifelong knowledge passport, educators could prepare a more individualized learning content and approach. The learner's knowledge passport provides the ability to predict the best teaching approach and select the right tasks in the right order. Emphasis on

the importance of a comprehensive view from strategic perspective on what and how learners will gain knowledge now makes it possible to evaluate progression and results between short-term gains in understanding and longer-term education goals. The proposed smart pedagogy blockchain is distributed between multiple education organizations, and it shares a single knowledge passport of the learner. Usually when an individual enters an education institution, there is a new, empty record to store the learner's assessment success. Upon an agreement between the learner and the education organization, all learning data would be available to the educator resulting in much more individualized learning content and approach. From scientific perspective, the knowledge passport not only boosts the learner's learning abilities but its analysis reveals more comprehensive trends about the learner, educator and the education organization. Such analysis based on empirical data would help to ask and answer new research questions.

2) Validation of learning result certificates. Like in the proposals discussed in the related research section of this paper, validity of learning evidence documents can be organized in blockchain architecture in multiple ways. If the documents reviewed stored validation data in cryptocurrency blockchains in order to meet smart pedagogy flexibility requirements, the author of this article proposes to build independent blockchain network shared among education institutions capable of smart pedagogy. Using independent blockchain designed primarily for education tracking purposes, allows learners, educators and education organizations to decide on the desired formats and processes without cryptocurrency framework limitations. In the next section of this paper, three nodes of an experimental network in different continents are connected using internet protocol over public internet. A notable part of national research and education organizations from Europe are connected to GÉANT network (GEANT, 2019). GEANT, the Gigabit European Academic Network, is a panEuropean data and communication network for Europe's education and research community. It is co-funded by education networks, European national research and the European Commission, and coordinated by a limited liability company DANTE. Across the European continent, the GEANT network provides research data communication, infrastructure and resources for telecommunication and information technology development. An organization connected to GEANT network, thanks to border gateway protocol on internet core smart pedagogy blockchain, would benefit from transit data flowing directly between interconnected education organizations.

Experimental setup and data structure

As in Fig.3, the experimental setup consists of three blockchain nodes located in Latvia, USA, and Singapore. All three nodes are logically fully meshed and physically connected via an internet protocol over public internet. If all nodes were connected in national academic institution networks with active GEANT connection, then blockchain data exchange would transit only GEANT network.

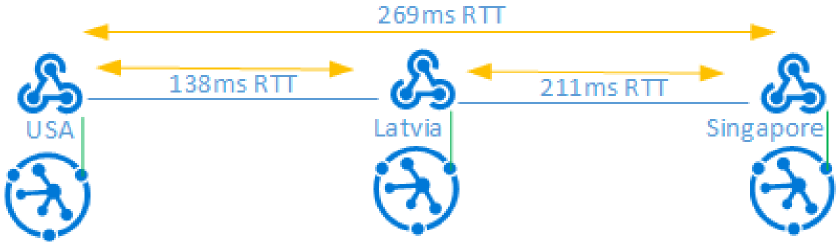


Figure 3. Blockchain node location and interconnectivity

All three blockchain nodes synchronize the blockchain database starting from genesis block followed by subsequent sequential blocks. The proposed architecture with three nodes is the smallest setup to demonstrate a decentralized peer-to-peer system with no central authority figure and quorum consensus. Blockchain nodes are located in different continents to observe real-life experience in realistic network for future smart pedagogy applications. Each node represents education institution and can append learners' achievements to blockchain as data in new blocks. After appending data to blockchain, it is not possible to delete or tamper with such data unless the whole blockchain is deleted. Depending on necessity, blockchain may contain not only academic or commercial final certificates issued at the end of learning process like degrees or professional titles but also more detailed assessment results on a subject or even topic level. Additional to digital certificate data, blockchain stores data creation timestamps. If the learner completed any assessment for the second time and results were published in blockchain, then all other nodes would have both the previous and actual assessment values for the same learner but with different timestamps. Considering future scaling, it is advised to store smart pedagogy centric data as links to education organization databases that get validated by corresponding hashes in blockchain network. However, it is possible to store smart pedagogy centric data also as raw data directly in blockchain for redundant storage on processing on other nodes. As in table 1, the proposed blockchain database architecture contains five columns where data field carries information about education organization, such as the creator, learner's profile, assessment type, result, timestamp.

Table 1. Proposed blockchain structure

index	previousHash	timestamp	Smart Pedagogy data	hash

Index – integer, e.g. 1;
previousHash and hash – double SHA256;
timestamp – unix timestamp, e.g. 1536851684.824;
data – varchar/string

Figure 4 shows general overview how smart pedagogy blockchain meets stakeholder interests. The learner demonstrates his/her gained knowledge through assessments. Recorded results for specific topics or subjects depending on an agreement between the learner and educator may be published as hashed smart pedagogy centric data in blockchain. Educators can access the learner's learning transcript and prepare appropriate methods and tasks to maximize the learner's learning abilities. When the learner has passed all assessments, education organization publishes a hashed digital certificate in blockchain. Once the digital certificate is published, the learner can share a link to the learning evidence to any third-party stakeholder who can directly validate the learners' success.

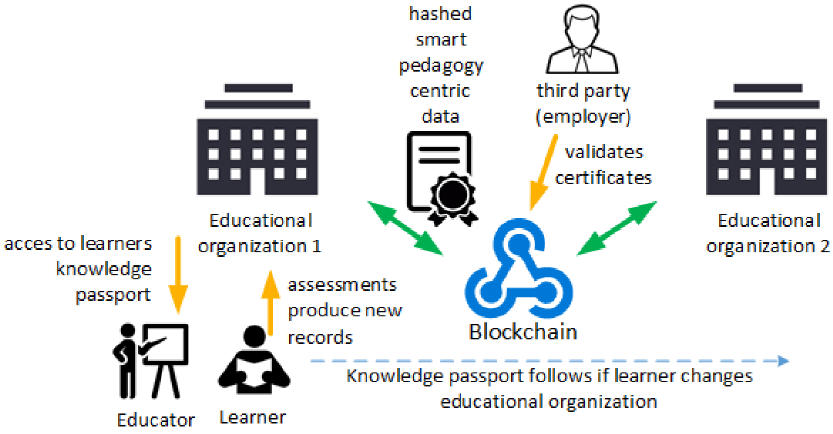

hashed smart pedagogy centric data
third party (employer)
validates certificates
Educational organization 1
Educational organization 2
acces to learners knowledge passport
assessments produce new records
Blockchain
Knowledge passport follows if learner changes educational organization
Educator
Learner

Figure 4. Smart Pedagogy blockchain stakeholders

The experimental process was divided in two steps. First, independent blockchain setup with three nodes and hashed digital certificate exchange. The main research question for the first experimental step was to answer what is difference between an independent blockchain approach compared to practice where certificate hashes are stored in blockchains of cryptocurrencies Bitcoin or Ethereum. As this proposed blockchain is designed only for processing smart pedagogy centric data, it has simpler and clearer database structure, and it performs better. During the experimentation, three imaginary education organizations generated 100,000 digital certificates each resulting in 300,000 digital certificate entries. Such volume of blockchain entries was chosen for comparison with Bitcoin daily transaction count (Blockchain Charts, 2019). With a single server blockchain solution in each node, it took approximately 3 hours, where average block confirmation time was approximately 20s compared to average 12 minutes in Bitcoin network in corresponding timeframe on June 26, 2019. On the other hand, Bitcoin network has more than 500,000 unique addresses and higher mining difficulty (Blockchain Charts, 2019). To sum up, independent smart pedagogy centric blockchain brings better performance and flexibility but will need more nodes to increase consensus quorum and security guarantees.

During the second experiment, the author generated and published 10,000 subjectbased assessment results on each blockchain node. Randomly generated data contained 100 educator id values and 1,000 learner id values on each node thus modeling a scenario where 1,000 learners in each educational organization get assessment in 10 subjects. Identification values of the education organization, educator, learner and the subject together with assessment result and timestamp were stored in a data field in blockchain. 30,000 generated entries were confirmed and distributed to all three nodes within 30 minutes. Now with available dataset, interested stakeholders can evaluate best students, best educators and analyze learners' knowledge passports and develop technology-enhanced learning innovations from smart pedagogy perspective. Transparency of success of learners and educators may lead to better rivalry among education organizations.

Results and conclusions

On the basis of experimentally collected evidence and dataset, the author concludes that blockchain architecture can be beneficial for the smart pedagogy domain as perspective to develop technology-enhanced learning innovations that use learners' lifelong knowledge passport. Although currently only minority of education organizations issue digital certificates instead of paper format learning evidence, author believes that in the future digital certificates will gain popularity. Depending on the choice of education institutions, digital certificates can be stored not only in cryptocurrency blockchains but also in specially designed blockchain for the education domain. The proposed blockchain architecture for smart pedagogy is in prototype state and for now can be used to demonstrate the idea of blockchain contributing to smart pedagogy and being another step in development of infrastructure with innovative benefits.

References

(2019, 06). Retrieved from SAP News Center: https://news.sap.com/2017/07/meet-truerec-by-sap-trusted-digital-credentials-powered-by-blockchain/

(2019). Retrieved from Blockchain Charts: https://www.blockchain.com/charts.

Bitcoin Transactions. (2019, 06 30). Retrieved from https://www.blockchain.com/btc/tx/f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16.

Blockcerts. (2019, 06). *The Open Standard for Blockchain Credentials*. Retrieved from https://www.blockcerts.org/.

Cachin, C., & Vukolic, M. (2017). Blockchain Consensus Protocols in the Wild. *Computer Science – Distributed, Parallel, and Cluster Computing*.

Contreras, A., & Gollin, G. (2010). The Real and the Fake Degree and Diploma Mills. *Change: The Magazine of Higher Learning*.

Daniela, L. (2019). *Didactics of Smart Pedagogy: Smart Pedagogy for Technology Enshanced Learning.* Cham: Springer.

Daniela, L., & Lytras, M. (2018). *Learning Strategies and Constructionism in Modern Education Settings.* IGI Global.

Finney, H. (2004). *RPOW – Reusable Proofs of Work*. Retrieved from https://nakamotoinstitute.org/rpow/.

GEANT. (2019, 06). Retrieved from https://www.geant.org/

Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Ferreira Torres, C., & Wendland, F. (2018). Blockchain for Education: Lifelong Learning Passport. *European Society for Socially Embedded Technologies*.

Haber, S., & Stornetta, W. (1991). How to Time-Stamp a Digital Document.

Learning Machine. (2019, 06). Retrieved from Certificates Verification: https://blockcerts.learningmachine.com/certificate/ab56912734bb5784bced00b7e0e82ac9.

MikroTik. (2019, 06 28). *Mikrotik Certificate search*. Retrieved from https://mikrotik.com/certificateSearch.

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

Nicosia, U. O. (2019, 06). Retrieved from Academic Certificate Verification: http://verify.unic.ac.cy/verify.

OpenZeppelin. (2019, 06). Retrieved from https://openzeppelin.org/.

Tapscott, D., & Tapscott, A. (2017). The blockchain revolution and higher education. *Educause Review*.

UNIC. (2019, 06). Retrieved from Masters in Digital Currency: https://www.unic.ac.cy/blockchain/msc-digital-currency/.