A Blockchain-based Educational Record Repository

Emanuel E. Bessa
Salvador University
Salvador, Bahia,Brazil
emanuel.bessa@hotmail.com

Joberto S. B. Martins
Salvador University
Salvador, Bahia, Brazil
joberto.martins@unifacs.br

ABSTRACT
The Blockchain technology was initially adopted to implement various cryptocurrencies. Currently, Blockchain is foreseen as a general purpose technology with a huge potential in many areas. Blockchain-based applications have inherent characteristics like authenticity, immutability and consensus. Beyond that, records stored on Blockchain ledger can be accessed any time and from any location. Blockchain has a great potential for managing and maintaining educational records. This paper presents a Blockchain-based Educational Record Repository (BcER²) that manages and distributes educational assets for academic and industry professionals. The BcER² system allows educational records like e-diplomas and e-certificates to be securely and seamless transferred, shared and distributed by parties.

Keywords
Blockchain; Security; Authenticity; Integrity; Distributed Ledger; Secure Transaction; Hash; Educational Record; Educational Repository; Educational Record Distribution.

1. INTRODUCTION
Blockchain is a technology considered by many to be something as relevant as the rise of the Internet. There have been experiments with blockchains since the early 1990's, but it was only in 2008, with the release of a white paper by an individual or group of individuals under the pseudonym of Satoshi Nakamoto, that blockchains gained wide adoption [9].

The first well-known blockchain-based implementation was the cryptocurrency Bitcoin [9]. Bitcoin is also the first widely-used, decentralized cryptocurrency. Basically, Blockchain technology is a shared peer-to-peer distributed ledger implementing a distributed database with some security characteristics.

Blockchain is a technology that may potentially support application development in many distinct areas. It is a peer-to-peer transaction management system without an intermediary. Blockchain allows transactions to be verified by a network of nodes and recorded in a public distributed ledger [2].

Educational records are used worldwide and, from the user point of view, is an important asset for individuals pledging for scholarships, jobs and professional and academic visibility in general.

In the educational context, a "certificate" is a type of educational record that represents an educational achievement or some type of relevant membership. University degrees, course and conference registers can eventually help individuals to get the job they want. In case you do not have a valid certificate, this may potentially prevent individuals from getting it. Currently, our educational records management systems are mostly physically localized, require specific and non-trivial procedures to access information, are in many cases unreliable and, finally, do not follow or have any educational standards.

Communication is currently available on a worldwide basis potentially allowing wide spread interactions and fostering visibility for citizens on various scenarios.

With the blockchain capabilities and citizen's global visibility perspective in mind this paper presents a Blockchain-based Educational Records Repository (BcER²). BcER² is intended to allow any individual to be able to store educational records and access multiple type of educational records with authenticity on a worldwide basis. It is a system to ensure educational records distributed management and access with inherent more security like authenticity and privacy.

This study focuses on the viability and benefits of Blockchain applied to the field of formal and non-formal education. In this way, Blockchain also represents an opportunity for the public to independently and privately verify that shared records are authentic and unadulterated.

In the next part of this article, section 2 summarizes the fundamental aspects of Blockchain technology. Section 3 indicates the relevant work being done related to Blockchain and BcER2system. Section 4 describes the architecture, entities, components and implementation of theBcER2system. Section 5 presents a proof-of-concept of the BcER² implementation. Finally, section 6 presents the final considerations and future work.

2. FUNDAMENTAL ASPECTS OF BLOCKCHAIN TECHNOLOGY
A blockchain is essentially a distributed database of records that keeps potentially all kind of data, like transactions, contracts and events. All information handling takes place across a peer-to-peer network and is maintained chronologically in digital blocks. These basic features and capabilities make Blockchain transparent, secure, decentralized and with almost unlimited storage capacity [4].

Chained blocks keep the history of all transactions made by the users since they access the system. As such, Blockchain can be also described as a register on which everyone can write, but cannot erase and/or destroy. As a result of using a peer-to-peer network, all copies of the records can be shared between the various computers known as "network nodes", consequently decentralizing the network and eliminating intermediaries.

Blockchain uses the concept of hashing. The "hash" is a block signature and considers all data and transactions involved. In summary, a cryptography hash function takes an input string and turns it into a unique n-digit string [9]. Figure 1 illustrates how blocks are chained in Blockchain.

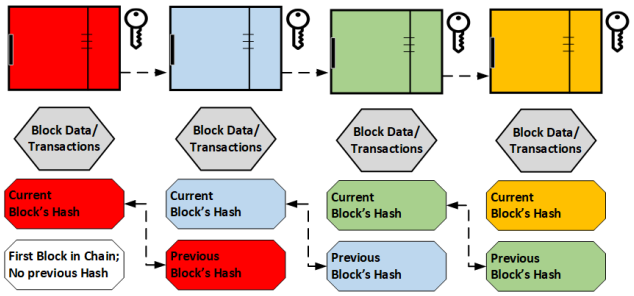

Figure 1. Blockchain basic operation.

2.1 Key Blockchain Characteristics

With traditional methods for recording transactions and tracking assets, participants on a network keep their own ledgers and other records. This traditional method can be expensive, partially because it involves intermediaries that charge fees for their services. It's clearly inefficient due to delays in executing agreements and the duplication of effort required to maintain numerous ledgers. It's also vulnerable because if a central system (for example, a bank) is compromised due to fraud, cyberattack, or a simple mistake, the entire business network is affected. To solve or improve traditional method Blockchain has a set of key characteristics: consensus, provenance, immutability and finality [9][2].

All relevant participants make decisions by consensus, in this process most participants must agree that a transaction is valid. This goal is achieved through the implementation of consensus algorithms. Each network enforces the conditions under which transactions are performed or the exchange of assets may occur. Provenance guarantees that participants know where the asset came from and how its ownership has changed over time. With immutability, no participant can tamper with a transaction after it has been recorded to the ledger. If a transaction is in error, a new transaction must be used to reverse the error, and both transactions are then visible. With finality, a single shared ledger provides one place to go to determine the ownership of an asset or the completion of a transaction.

2.2 Why "Blockchain" to Manage and Improve Visibility for Educational Records

An "education record" in the context of this paper is a record containing files, documents, and other materials which [9]: i) Contains information directly related to the academic historical of a student or a professional; and ii) From a local perspective are typically maintained by an educational institution or by other entity acting for such institution.

There are significant advantages and benefits in using a Blockchain-based educational repository [3] [17]: i) Educational records (e-diplomas, e-certificates, other) uploaded and managed on the Blockchain ledger are more secure and resistant to "physical wear and tear" than paper documents [3]; ii) Educational records are seamless and efficiently transferred and shared among parties (universities, schools and employers) fostering worldwide visibility; and iii) Educational records stored on the blockchain can be accessed any time, from any location.

3. RELATED WORK

In recent years, blockchain technology has been widely used as the basic construct for crypto-coins such as Bitcoin [15] For some experts this is considered the first generation of Blockchain. The use of Blockchain in this sense has grown considerably and it is currently estimated that there are over 1600 crypto-coins. [15].

MIT has a system for building Blockchain-based applications that issues and verifies official records called "Blockcerts Wallet". It allows, for instance, the creation of a certificate wallet for students to receive virtual diplomas via their smart devices [13]. Different from Blockchain-based Educational Records Repository (BcER²), MIT Blockcerts Wallet system is a building application platform that has a similar target in terms of allowing educational records creation and dissemination using Blockchain.

New promisingly Blockchain-based solutions include 'intelligent contracts' [14]. Ethereum, discussed in [16], allows the creation of contracts that are self-managed. Contracts are triggered by an event such as passing an expiration date or achieving a specific price goal. In response, the smart contract manages itself by making adjustments as needed and without the input of external entities [1]. Blockchain utilization for automated smart contracts dealing with energy transactions for the Smart Grid is discussed in [14].

As time went on and the hype of the cryptocurrencies passed, developers began to realize that Blockchain could do more than simply manage 'document transactions'. Jurdak et al. in [6] discusses Blockchain adoption for privacy and security support in the Internet of Things (IoT). Blockchain cybersecurity and privacy performance vis-a-vis cloud solutions is discussed in [11]. Barguil et al. in [5] discuss how blockchain technology and smart contracts can improve data access, data management and data interoperability of Electronic Health Records (EHR). Potential Blockchain application towards innovation in Smart Cities are discussed in [7]. Blockchain applications for supply-chain to validate individuals and assets are introduced in [10]. A mobile edge computing enabled Blockchain system is presented in [18] to allow its application in mobile services where computational capability is limited.

Blockchain deployment may have problems like scalability and required processing power [19] [6]. Some of the effort made by researchers and developers in the area will be in solving scalability and processing capability problems, thereby giving more applicability to Blockchain technology.

4. THE BLOCKCHAIN-BASED EDUCATIONAL RECORDS REPOSITORY (BCER²) - ARCHITECTURE AND COMPONENTS

In order to meet the different alternatives of use, blockchain-based applications can be implemented using 3 types of general structures as follows [2]: i) Public Blockchain; ii) Private Blockchain; and iii) Consortium Blockchain.

The type of Blockchain structure to be used strongly depends on the application. The BcER² repository adopted the consortium system since only authorized persons are able to create certificates records on the network. On the other hand, anyone can verify their authenticity. Thus, when registering an educational record, for example, the responsible for creating the record writes in the registry or in the database using its own private key. Users who want to check the veracity of the record must have a corresponding identifier number to be inserted into the system.

The public Blockchain arose from the need for a totally decentralized blockchain structure that allows open use, reading and participation in the management of operations within the network. The main feature of this model is the secure protection of users.

The private Blockchain owns its business network written and developed by a centralized organization. The company writes and verifies each transaction, in addition to deciding the network read permissions. This increases efficiency, enhances user confidentiality, and reduces transaction costs. All the autonomy on the part of the organization constitutes its main characteristic.

The Blockchain consortium is a semi-private and partially decentralized chain system, in this scenario the nodes are responsible for the validation of the transactions and how this happens depends on the implementation of the consensus methods. The form of access and consultation of the records can be public or private and the owner of the network is responsible for its configuration.

The BcER² effective structure uses the basic steps and operation flow of a blockchain-based application as illustrated in Figure 2 i) A transaction is requested by someone who has prior authorization and needs to create an educational record; ii) The request record transaction is sent to the nodes belonging to the BcER² system; iii) The educational record transaction is verified by the ledger; and iv) A new block of data corresponding to the educational record transaction is accessed or created and annexed to the ledger becoming permanent and immutable completing the transaction.

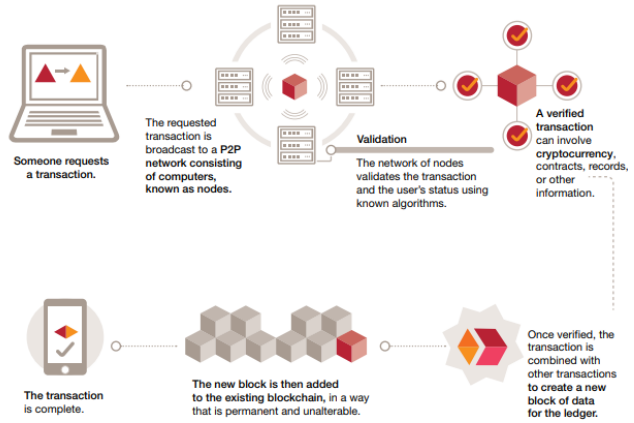

Figure 2. BcER² basic steps and flow operation - Figure available at [2].

4.1 Blockchain-based Educational Records Repository (BcER²) Entities

The entities belonging to the BcER² educational repository are the following: i) Assets; ii) Registers; iii) Transactions; and iv) Participants.

An "asset" can be anything of value that will be kept securely by the educational repository. Educational records like certificates, diplomas, educational records an similar documents are BcER² assets.

"Participants" are the educational organization representatives, students and people in general that are somehow interested in either distributing or accessing educational records. Participants are defined in the "business network model" adopted by the blockchain application process. For BcER², coordinators, students, and anyone else interested in having access to the educational records are the participants belonging to the network. Each one has their specifically assigned functions, responsibilities and access restrictions.

"Transactions" are submitted by participants to create or access the assets held in the blockchain-based asset registries on the blockchain ledger. Transactions, in general, do belong to a business network and, as such, do require a "business network model". The business network model, from the blockchain system perspective, define the operation involved with the assets.

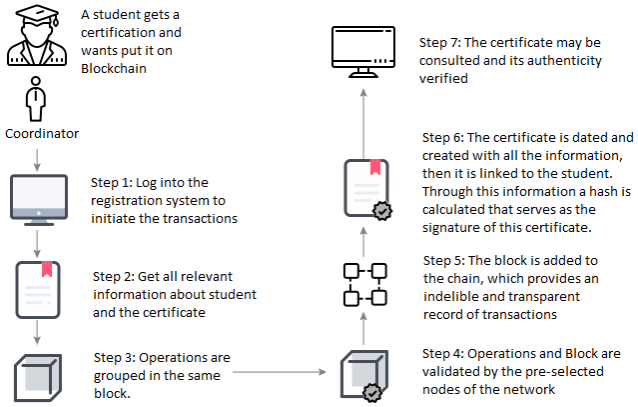

Figure 3. "Certificate Register" creation in BcER².

"Registers" can be defined as the set of data that involve the assets, transactions and the participants. this set is what will be included in the block after the validation. Registers are new information that is added to the blockchain ledger.

In BcER² educational records repository the addition of a "register" is carried out through the execution of steps. In these steps, the business model adopts the following "business" premises: i) The course coordinator or the educational institution representative are the authority to create new assets; and ii) Students and general public are participants that access the validated and secure educational assets maintained by the system.

The creation of a register is executed as illustrated in Figure 3: i) A coordinator proceeds to write a record to the Blockchain account, which means create the certificate with an identifier. In this process the coordinator selects the certificate and through its identifier number it is possible to link it to a student; ii) The record is saved and time-stamped in a block using arithmetic operations; iii) The block is subsequently validated by network pre-selected nodes through cryptography techniques; and iv) The block is dated and added to the block chain, so that all users can have access to the same chain since each node builds its own exemplary independently.

Once these steps have been executed, we can access educational records with authenticity and integrity by simply using a credential (ID Card) through a web browser.

4.2 Blockchain-based Educational Records Repository (BcER²) Business Network

The business network is a fundamental definition for the BcER² educational registry repository deployment.

In summary, it models the BcER² "educational model", defining the existing assets, transactions and participants related to them. The business network defines the transactions that

interact with assets. The model also includes the definition of participants who interact with assets and associates a unique identity, across multiple business networks. As described before, BcER² is composed of assets, participants and transactions, with each of these entities modeled in relation to the educational operation.

4.3 Blockchain-based Educational Records Repository (BcER²) Components

The basic components belonging to the BcER² educational records repository are illustrated in Figure 4 and basically reflect the business network adopted which is suitable for an educational records repository that registers, manages and provide access to them.

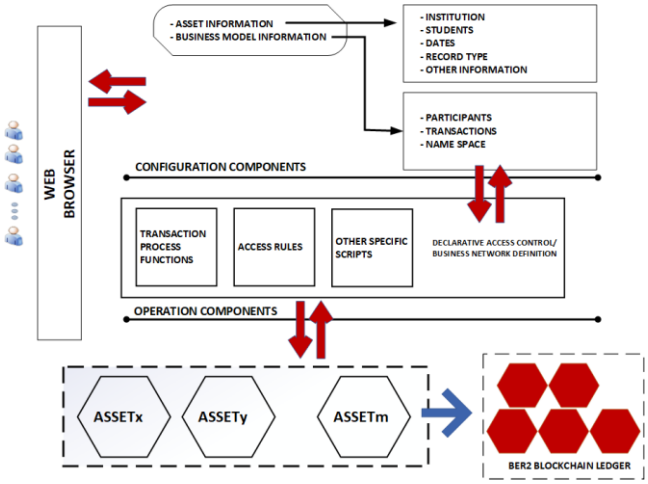

Figure 4. BcER² basic components.

The "asset information" component contains information related to the educational record being managed by BcER². This component is responsible for asset's definition and consistency.

The "Business Model Information" component contains information related to the process involved in the asset management. It defines basically the participants, name space and transactions involved in the process.

The "Transaction Process Function" component contains the information concerning the specific functions invoke in the business model to manage the asset.

The "Access Rules" component contains, as the name suggests, the access rules including all priorities among participants involved in the business model adopted.

BcER² managers and general users access the repository through a web browser using identification cards (ID Cards) which includes connection profiles and credentials.

Assets are effectively deployed in the BcER² blockchain ledger in this specific system by the Hyperledger Composer framework described in section 4.4.

4.4 Blockchain-based Educational Records Repository (BcER²) Implementation

The Hyperledger Composer [8] was used to implement the BcER² educational repository (Figure 5). Hyperledger Composer is an open source development tool set and framework aiming to support the development of blockchain applications. It allows the modeling of the business network and integrates existing systems components and data deploying as such the blockchain application.

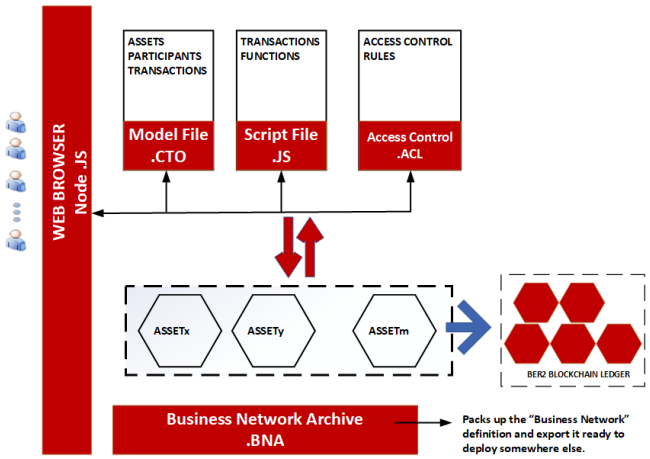

Figure 5. Hyperledger Composer deployment.

The use case adopted by the actual implementation is initially intended to verify the authenticity of student's certificates generated by Salvador University (UNIFACS) under-graduation courses.

BcER² is composed of assets, participants and transactions, with each of these entities being represented within Hyperledger framework as configuration files (Figure 5).

The .CTO Hyperledger component is responsible for implementing the assets, participants, and transactions, including all relevant information. A Hyperledger Composer CTO file is composed of the following elements: i) A name-space with resources declaration; ii) Resources definition including assets, transactions, participants and events; and iii) Optional resource import declarations from other name-spaces.

The .ACL Hyperledger component provides declarative access control for the elements in the domain model. By defining access and control (ACL) rules you can determine which users/roles are permitted to create, read, update or delete elements in a business network's domain model.

The 'Business Network' definition, from the Hyperledger Composer perspective, is composed by a set of model files defining assets, participants and transactions (Figure 5). The ".JS" script file is responsible for maintain a set of scripts. The scripts contain transaction process functions that implement the transactions defined in the 'Business Model'. Transaction processing functions are automatically invoked at run-time when transactions are submitted and their structure are composed by a JavaScript function.

5. BCER² REPOSITORY - PROOF-OF-CONCEPT

The main objective of the BcER² repository proof-of-concept is to validate the deployment of the business network and verify the operation steps of the repository by: i) Creating assets; and ii) Accessing them and verifying the effectiveness of credentials and other distribution and security aspects.

The proof-of-concept of the BcER² repository operation was implemented by emulating participants as follows: i) 'Users' are the general public accessing educational records; and ii) The 'Coordinator' (Register Authority) is a UNIFACS authority creating educational record entries.

The experiment was executed using the following infrastructure: i) The BcER² system runs on Notebook Core i7, 2.0 Ghz, 8 GB RAM, Ubuntu Server Operating System 16.04 x64; and ii) The coordinator and users access the BcER² system using any browser.

The software components installed to run the BcER² system are i) Node Version 8.12; ii) NPM Version 6.4.1; iii) Visual Studio Code Version 1.28; iv) Docker Engine Version 18.06; and v) Docker Composer Version 1.23.

The proof-of-concept method and parameters used to validate the operation of BcER² was the creation of a set of educational records followed by authenticity verification and access by the system administrator and distributed users. The experimental setup included the creation of 10 different educational records with course certificates and various nodes (N>10) simulating different users acting on the validation process (transactions) and verifying their authenticity. The results allowed the distributed access to educational records enabling verification through blockchain technology. Security access was also validated by trying to access educational records without the adequate credential. The scalability of the solution was not evaluated and will be addressed by future work.

6. FINAL CONSIDERATIONS AND FUTURE WORK

New technologies have always attracted companies and governments. This is largely due to the promise to improve the current way of working and providing services. Blockchain technology is a new strategy that gives users great possibilities of use. This technology has demonstrated great potential with the possibility of eliminating intermediaries, besides having great advantages such as security, transparency and confidentiality of the users. This is offered by a database similar to a registry, implemented in a shared way between all nodes in a network. Most experts agree with its potential and Blockchain technology is being applied and new use cases are being implemented every day.

We propose in this work to use Blockchain technology as a tool to provide a secure and efficient way to access certificate with authenticity. We argue that the proposed Blockchain BcER² repository has the potential to support the education sector by providing better support for certificate management and distribution.

In the current scenario, the proposed application covers only the UNIFACS network for the purpose of managing diplomas and certificates issued by the university. The BcER² application has the potential to cover additional areas in which digital certificates provide interesting opportunities such as [12]: i) Corporate Training - Many large companies offer a multitude of training opportunities to their employees, but lack the systems to track and store results reliably. Current human resources systems often do not interact with corporate databases and there are no consistent standards for comparing skills and accomplishments; and ii) Workforce Development - There are millions of records and learning certificates, but there are no systems to manage them. This is especially a problem for people with low qualifications, who often do not have recognized diplomas or degrees.

In terms of future work, it is intended to evaluate the scalability issues and impacts associated with the deployment of a huge repository. Another aspect to be considered is to bring together stakeholders such as employers, students, teachers and contractors in a way that they interact with each other enabling wide-spread use of trustable e-certificates. A final target will be to adopt a fully standardized asset representation as an additional step towards a secure and decentralized way of conferring a wide-spread use of the system.

7. ACKNOWLEDGMENTS

Authors thanks FAPESB (Fundação de Apoio à Pesquisa do Estado da Bahia) by the scientific initiation (IC) scholarship support.

8. REFERENCES

[1] Habib Azam. What are the different generations of blockchains? Jan. 2018. url:https://medium.com/@habs/what-are-the-different-generations-of-blockchains-bebf3c3ad57f (visited on 11/16/2018).

[2] Sanjaya Baru. “Blockchain: The next innovation to make our cities smarter”. In: (Jan.2018), p. 48.url: https://www.pwc.in/publications/2018/blockchain-the-next-innovation-to-make-our-cities-smarter.html.

[3] Institute of Blockchain. Blockchain and Education. June 2018.

[4] Michael Crosby. “Blockchain Technology: Beyond Bitcoin”. In: 2 (2016), p. 16.

[5] Arlindo F. da Conceição, Flavio S. Correa da Silva, Vladimir Rocha, Angela Locoro, and João Marcos M. Barguil. “Eletronic Health Records Using Blockchain Technology”. In: Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações - WBlockchain - SBRC 2018. Vol. 1. SBC - Brazilian Computer Society, May 2018.

[6] Ali Dorri, Salil S. Kanhere, and Raja Jurdak. “Towards an Optimized Blockchain for IoT”. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation. IoTDI ’17. New York, NY, USA: ACM, 2017, pp. 173–178.isbn: 978-1-4503-4966-6.doi:10.1145/3054977.3055003.

[7] FICCI and PwC India. Blockchain: The Next Innovation to Make Our Cities Smarter. https://smartnet.niua.org/content/d18d3972-ff71-4ce8-af03-6079f1849bd5. 2018.

[8] Linux Foundation. Introduction — Hyperledger Composer.url: https://hyperledger.github.io/composer/latest/introduction/introduction (visited on 11/16/2018).

[9] Alexander Grech and Antony F. Camilleri. Blockchain in Education. Tech. rep. EUR28778 EN. Luxembourg: European Union, 2017, pp. 1–136.doi:10.2760/60649.

[10] Nir Kshetri. “Blockchain’s Roles in Meeting Key Supply Chain Management Objectives”. In: International Journal of Information Management (Apr. 2018), pp. 80–89 ISSN: 0268-4012. doi:10.1016/j.ijinfomgt.2017.12.005.

[11] Nir Kshetri. “Blockchain’s Roles in Strengthening Cybersecurity and Protecting Privacy”. In: Telecommunications Policy. Celebrating 40 Years of Telecommunications Policy – A Retrospective and Prospective View 41.10 (Nov. 2017), pp. 1027–1038.issn: 0308-5961.doi: 10.1016/j.telpol.2017.09.003.

[12] MIT Media Lab. Certificates, Reputation, and the Blockchain. Oct. 2015.url: https://medium.com/mit-media-

lab/certificates-reputation-and-the-blockchain-aee03622426f(visited on 11/16/2018).

[13] MIT Media Lab. What we learned from designing an academic certificates system on the blockchain. June 2016.url: https://medium.com/mit-media-lab/what-we-learned-from - designing - an - academic - certificates - system - on - the - blockchain -34ba5874f196(visited on 11/16/2018).

[14] M. Mylrea and S. N. G. Gourisetti. “Blockchain for Smart Grid Resilience: Exchanging Distributed Energy at Speed, Scale and Security”. In: 2017 Resilience Week (RWS). Sept.2017, pp. 18–23.doi:10.1109/RWEEK.2017.8088642.

[15] Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”. In: (2008), p. 9.

[16] Nathan Reiff. Blockchain Technology’s Three Generations. en. July 2018.url: https: //www.investopedia.com/tech/blockchain-technologys-three-generations/ (visited on 11/16/2018).

[17] Raza Sheeraz. Blockchain Can Help People Keep Their Educational Records Intact. US.May 2018.

[18] Zehui Xiong, Yang Zhang, Dusit Niyato, Ping Wang, and Zhu Han. “When Mobile Blockchain Meets Edge Computing”. In: arXiv:1711.05938 [cs] (Nov. 2017). arXiv:1711.05938 [cs].

[19] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. “Where Is Current Research on Blockchain Technology? —A Systematic Review”. In: PLOSONE11.10 (Oct. 2016), e0163477.issn: 1932-6203.doi:10. 1371 / journal. pone .0163477.