Leo Mrsic, Goran Fijacko and Mislav Balkovic

2 Digital identity protection using blockchain for academic qualification certificates

Abstract: Although it was always an important issue, digital era increases the importance of both questions “what identity is” and “why is important to manage and protect one.” There are many views and definitions of digital identity in the literature; however, this chapter explains the identity related to the identification of an individual, his/her qualification, and his/her status in society. Using modern approach, this chapter focuses on the academic qualification of an individual where blockchain is presented as an efficient concept for publishing, storing, and verifying educational certificates/diplomas. Motivation for this research came from lack of practical applications of blockchain and importance of EDU certificate transparency and challenges in their sharing (policy issues, national standard, etc.). By having easy to apply and understand guidelines, it is easier for wider audience to accept and use/reuse sometimes complex digital concepts as part of their solutions and business processes. As part of institution research lab, explained approach and proof of concept solution was developed in Algebra University College.

Keywords: digital identity, blockchain, smart contracts, academic qualification certificates, certificate Mrsic, Fijacko and Balkovic

2.1 Introduction

If we talk about a classical identity of an individual, we can think of personal identity card, a birth certificate, a driving license but also a university certificate/diploma or other EDU certificate. In terms of the digital identity of an individual, we can talk about an e-personal ID card, e-birth certificate, e-homepages, e-driver’s license or e-diplomas [1]. The e-name tag is electronic, which means these documents also have a digital component. This digital component can be, for example, an electronic data carrier (chip) that stores certain data or certificates that are readily uploaded to the computer by a reader if needed. The data being displayed are centralized and are guaranteed by and responsible to the institution issuing them, where the data is stored [2].

Digital identity does not necessarily have to be a physical document or document [3]. It also includes our email addresses as well as various user accounts and

Leo Mrsic, Goran Fijacko and Mislav Balkovic, Algebra University College, Croatia, Europe.

profiles on the Internet, such as an eCitizen account, Facebook profile, and email (Figure 2.1).

Figure 2.1: Authentication process (adopted from Phil Windley, Digital identity, p. 37).

Blockchain is one of the disruptive technologies that are often called technology, which will change the world and enable a new revolution. Blockchain represents a decentralized database that is publicly available to everyone via the Internet. Take for example databases and registers owned by the state and its institutions such as ministries, banks, and mobile operators, and all listed registers and data are published publicly by placing them in the blockchain. It allows us to access all data concerning our own, with authorization and access to the Internet. Likewise, we can present the same information to the other side as soon as we need to prove their identity, valid information or some information.

2.2 Smart contracts

With the help of smart contracts in the blockchain you can enter a program code or even entire applications. Smart deals define the relationships and behavior of two or more sides in the blockchain that have some cryptocurrency or some other information

or value. With this type of blockchain technology, there is a possibility that in the future there will be no standard services of attorneys, commercial courts, public notaries, and the like. A good part of the services they currently offer is likely to be easily replaced by smart deals because the relationship between the users and the providers of the above-mentioned services can be precisely defined through the code and entered into smart deals that are later realized by meeting all the conditions within the transaction. Realization of the services is automated and extremely fast, which in today's form is not. The use of smart deals allows the exclusion of a whole range of mediators in different processes and thus enables faster and easier to perform activities, private, and more importantly, business. They can be used, for example, in the following:

- **Under insurance:** If authorized agents in the blockchain register that the conditions for the payment of the insurance are met, the payment will be automatically made.
- **Medical insurance:** If a doctor finds that a patient is ill and unable to complete his/her business obligations, blockchain inserts that information, and the patient automatically starts to pay the sickness benefit.
- **Pension insurance:** If an authorized person or a state body certifies that a person has fulfilled the retirement conditions, a person will automatically be paid a pension.
- **Audio and video industry:** If a user pays for viewing or listening to a certain material, he/she automatically gets access to and rights to the purchased material.
- **Gambling industry:** The user who makes a bet is paid into the account of a smart contract. After the event is complete, the authorized party registers the data on the winner in the blockchain and those who successfully hit the results automatically receive payments.

2.3 Digital identity protection

Identity is very valuable to us, and not to institutions; we are not behaving accordingly [4]. The lack of awareness and education about importance of identity protection in digital world, powered with centralization of databases that store data about identities in general, represents unavoidable weakening trend that undermine the systematic value of our personal data. Centralized systems are a good booty for attackers with bad intentions because, if they break into the system, they can easily steal (copy) large amounts of data stored in that system. We have witnessed a lot of attacks on centralized systems, not small business systems, but big and globally influential companies such as Yahoo, eBay, Adobe, JP Morgan Chase and Sony.

Blockchain technology offers the solution to this problem that is becoming more and more constant due to constant needs, increased demand, and the use of digital identity. But, as we mentioned earlier, this is a new technology and is just in

the early stages of the project and we are still investigating all the possibilities and the application of this technology [5].

With the need to prove our identity, we meet each day and in different places: at work, in a bank, in a shop, in travel, in state institutions, and in many different places [6].

Currently, there are many new and prospective projects and young companies dealing with this problem and are trying to find their place in the market. In this part, we will mention some of them and more specifically explain their business models.

2.3.1 Civic

Civic is a company that develops an identification system that allows users to selectively share identifying information with companies. Their platform has a mobile application, where users enter their personal information and then store them in encrypted format. The company's goal is to establish partnerships with state governments and banks, that is, all those who can validate user identity data, and then leave a verification stamp in blockchain. The system encrypts the hash of all verified data and stores it in the blockchain and deletes all personal information of the user from their own servers.

As the company has written in its White Paper, the Civic Ecosystem is designed to encourage the participation of trusted authentication bodies called “validators.” “Validators” can be the aforementioned state governments, banks, various financial institutions, and others. As Civic currently validates user identity information through its application, “validators” have the ability to verify the identity of an individual or a company that is “user” of the application. They then affix the certificate and place it in a blockchain in the form of a record known as attestation. This “verification” is actually a user's hash of personal information. Parties known as ‘service providers wanting to verify the same user identity data should no longer be able to independently verify that information but rather use the verified information valid for those validators of that information. The goal is to remain a “ruler” of your identity and to have full control over personal information so that it must give prior consent to each transaction of information about its identity between the validator and the service provider. By smart deals, validators have the ability to sell their approvals to service providers, but also to service providers to see at what prices different validators offer their approvals. Each validator can declare the price it is willing to sell personal user information. After the user, validator and provider confirm the transactions through the smart deal system, the service provider pays the validator the required amount in the form of CVC tokens (utility tokens that support decentralized identity ecosystem supported by Civic's model which allow on-demand, secure and lower cost access to identity verification via blockchain). After that, a clever contract will allocate CVC tokens and the user will get their share of the participation. The user can use their tokens to purchase products and services on

the Civic platform. As we mentioned, the user is the one who is responsible for their data and stores them on some of their personal devices using the Civic app, and it is also recommended to back up a personal account on the cloud system. Since user identity data is not centralized, that is, not on Civic servers, there is no possibility of massive identity theft since the data of each user is actually on their devices and that data will be stolen, so it is necessary to break it into each device separately. This information largely helps to suppress the black market for personal information, for example, Black credit card market is quite widespread because transactions can only be done by knowing these data without the knowledge of the user. If a credit card number needs to go through the blockchain mechanism of proofing where the user's consent for each transaction should be, then the black market of such data slowly loses its meaning and value (Figure 2.2) [7].

Figure 2.2: Civic concept.

2.3.2 HYPR

HYPR is a young company, founded in 2014. Their business model is based on merging biometric identification methods and blockchain technology. Biometric identification can replace a classic identification with a username and password, which is faster and

safer. Biometrics can recognize different parts of the human body such as palm geometry, fingerprint, eye iris, scent, face, and many long physiological elements unique to the individual. Biometrics is a very good way of verifying an individual's identity because it is very difficult or impossible to forge it.

HYPR therefore offers a password-free authentication platform with biometric encryption. The company does not deal with the development and production of identification devices, but develops a distributed security system. As mentioned earlier, every digital data can be used to insert some of the cryptographic algorithms and get their hash. This hash can be used to validate these digital data without the need for a validator to have a copy of that data. For example, we read our finger on a fingerprint reader on a mobile phone, and a company that has access to the hash of our fingerprint in digital form can confirm our identity, without the possibility of being false as we do. Digital print is just a part of the offering that is offered. HYPR supports many types of biometric data, from simple authentication algorithms to face and speech algorithms to much more complex algorithms such as keyboard typing, rhythm writing on mobile devices, or the way we walk. With blockchain and data decentralization, authentication becomes much faster and simpler. Each user is responsible for their biometric data, such as on his mobile device. This avoids massive data theft, while individual theft may still be possible if the user is not careful enough to protect their data and devices. Such a system based on blockchain technology is resistant to denial of service (DoS), which is a better centralized system. DoS attacks are attacks on some computer service in order to disable its use. In this case, instead of attacking a single server used to authenticate data, DoS attackers should identify and attack all blockchain nodes in that system. The company emphasizes that protecting against DoS attacks is equally important and the interoperability of business processes. There is currently no possibility of authentication between two different corporate entities such as a bank and an insurance company. Each company has a different identity database and they are not interoperable. Using blockchain technology, we can have an interoperable distributed mainstream identity book between multiple entities without the need for complex and expensive infrastructure. Thus, the insurance company can prove our identity to the bank through biometric data [8–10].

2.3.3 Blockverify

The problem of proof of identity does not only appear in people. It may also be present in various products such as medicines, luxury products, diamonds, electronics, music, and software. These products are often counterfeit, causing damage to manufacturers in billions of dollars.

People behind the Blockverify project want to reduce the number of counterfeit products on the market by preventing duplicate appearances. Different companies

from different industries can register and track their products using Blockverify and blockchain technology.

The company believes that improvement in counterfeit products can only be achieved by using decentralized, scalable, and safe solution attacks. Blockverify has its own private blockchain, but it also uses Bitcoin's blockchain to record important changes in its chain. Their chain is highly scalable and transparent so that each manufactured product can enter into it as an asset. After that, each of these assets will be added to the blockchain and assigned a unique hash. Anyone with that hash can access blockchain and check whether the product is valid or not. The primary goal of the company is to address the problem of counterfeit medicines, which is first on the scale of counterfeit products, but also one of the more dangerous counterfeit products because it directly affects people's health and causes millions of deaths per year. Another problem that a company wants to solve is the problem of verification of ownership. Thanks to blockchain technology, ownership changes can be easily recorded permanently. By this mode, individuals are prevented from making duplicate records and unauthorized changes.

2.4 Digital identity and blockchain

The main features of blockchain are transparency and decentralization, which today's systems cannot boast. Digital identity combined with blockchain technology will enable people to perform tasks that are faster, simpler, and safer, including proof of identity, facts, status, and data. Incredibly, the fact is that searching for new employees, checking candidate data, and job application itself could be a process that would take just a couple of mouse clicks on the computer, with the utmost certainty of the data being obtained [11]. But blockchain is just offering it. By placing all the information on our identity on it, with cryptography that makes the whole thing safe and transparent and always accessible through the Internet, we spend all the time spent on proving identity, data, facts, and state of affairs on the most important things. Imagine that we can also enclose three cryptographic keys with the application for business, so that the employer can easily check with the absolute certainty that we have actually completed the college we have stated in his CV, whether we are unhappy and whether we are at all a person who claims to be [12]. This process would take about a few minutes, while the same process lasts for several days, if not weeks, as the data verification is done by writing queries in each of these systems from which data comes [13, 14].

Blockchain got its name by the way it stores the transaction data that is happening. It stores them in blocks that together form a chain.

By increasing the number of transactions being made, the size of the chain in which they arise increases (Figure 2.3). The blocks record the sequence and time of

Figure 2.3: Showing transactions stored in blocks that connect each other to a chain (Source: Gupta, M., *Blockchain for dummies*, 2nd IBM Limited Edition, 2018, p. 14th).

the transactions that are then recorded in the network chain according to certain security rules agreed between the participants. Each block contains a hash, that is, a digital imprint or unique identifier, then time-tagged valid transactions and hash of the previous block. Hash of the previous block mathematically links the blocks to the chain and prevents any change of data and information in the previous blocks or inserting new blocks between the existing ones. Thus, each of the following blocks increases the security of the entire chain and reduces the already small chance of manipulation and change of value or data in the chain.

There are several types of blockchains. In this chapter, we will mention the two most common types:

A public blockchain, such as Bitcoin blockchain (the first and most known cryptovalue based on this technology), is a large distributed network that runs with the release of a native token. The public blockchain is visible and open to everyone to use at all levels. An open code is maintained by the developer community.

Private blockchain is smaller in volume and usually does not run with token issuance. Membership in this type of blockchain is highly controlled and is often used by organizations that have confidential members or traded with confidential information.

All types of blockchains use cryptography to enable each participant to use the network in a safe manner, and most importantly, without the need for a central authority that applies the rules. Because of this, blockchain is considered revolutionary because it is the first way to gain confidence in sending and writing digital data.

An example, my name text, Goran, passing through the SHA-256 algorithm gives the result

dbe08c149b95e2b97bfcfc4b593652adb8586c6759bdff47b533cb4451287fb

The word Goran will always result in an identical hash value. Adding any character or letter at the input changes the complete hash appearance, but of course, the mentioned 32-character length always remains the same. An example, word Gordan, gives the result

dbe08c149b95e2b97bfcfc4b593652adbf8586c6759bdf47b533cb4451287fb

In addition to the mentioned blocks and chains that are interconnected, there is another very important segment, which is a network. The network consists of nodes and full nodes. The device that connects and uses a blockchain network becomes a node, but if this device becomes a complete node, it must retrieve a complete record of all transactions from the very beginning of the creation of that chain and adhere to the security rules that define the chain. A complete node can lead anyone and anywhere, only the computer and the Internet are needed. But that's not so simple as it sounds.

Many people mix Bitcoin and Blockchain concepts or misuse them. Those are two different things. Blockchain technology was introduced in 2008, but it was only one year later launched in the form of cryptocurrency Bitcoin. Bitcoin is therefore a cryptocurrency that has its blockchain. This blockchain is a protocol that enables secure transmission and monitoring of cryptocurrency Bitcoin, all from the emergence of its first block (genesis block) and the first transaction. Bitcoin is designed solely as a criterion of vision that one day completely replaces fiat (paper) money and crushes the money transfer barriers that are present today. Through the years that passed, the community found that blockchain is more powerful than it originally thought, so if Bitcoin as a cryptocurrency does not live globally in everyday life, it will leave behind a revolutionary invention that potentially can change the technological world we are currently familiar with.

Blockchain through its mechanism of consensus eliminates the central authorities that we know today and which are based on today's technology.

2.5 Platform: issuing EDU certificate

MultiChain was selected as the platform for creating an application concept for entering, issuing, and verifying educational certificates. MultiChain is an open-source platform that allows you to create or block your own blockchain, and manage its capabilities. It is optimized for creating licensed chains (permissioned blockchains). MultiChain is compatible with Linux, Windows, and Mac operating systems. Currently optimized for Linux operating systems, here referred to as Linux's 64-bit Ubuntu 18.04.1 operating system with virtual machine on a single physical server using Oracle VM VirtualBox.

Virtualization of operating systems enables us to have multiple operating systems on one server, workstation, or computer, and we use them at the same time. All operating systems share computer resources. The number of virtual machines is unlimited, that is, it depends on the amount of disk space and the memory of the computer hosted on.

In the Oracle VM VirtualBox workstation there is a File, Machine, Help, icons for the most important activities on virtual machines (New, Settings, Discard, Show), and below them there is a window where show installed virtual machines, including Ubuntu's virtual machine, with assigned 100 GB of disk space and 3 GB of work memory. Before installing the operating system, it was necessary to create a virtual disk of the specified size that the machine would use.

The complete work console and virtual machine installation is very intuitive and simple. VirtualBox offers the ability of detachable virtual machine start-ups, enabling the entire process to run without open windows and a graphical user interface.

After installing and configuring a virtual machine, we must download and install the MultiChain application. Download, install, and all other actions within MultiChain are performed through the Terminal of Ubuntu Operating System Interface. The following commands are used to download and install:

```
wget https://www.multichain.com/download/multichain-1.0.6.tar.gz
tar -xvzf multichain-1.0.6.tar.gz
cd multichain-1.0.6
mv multichaind multichain-cli multichain-util /usr/local/bin
```

The last command line transfers the most important files to the bin folder for easier calling through the commands in the next steps.

After installing the MultiChain application, the first step is to create your own chain. Since the goal of the application is to enter, issue, and validate educational certificates for the purpose of this project, we called the chain BlockchainCertificate. This is done by performing the following function:

```
multichain-util create BlockchainCertificate
```

Using this command, we create the chain of this name with the default settings. After that, you must launch the created chain using the following command:

```
multichaind BlockchainCertificate -daemon
```

The chain was launched and its first block (genesis block) was created. After launch, the newly created chain gets its IP address and port through which it can be accessed from another device. The device on which the chain is created becomes

the first node, and each subsequent computer that connects to that chain over its IP address and the default port receives the complete chain data and also becomes a node. For the purpose of this chapter, only one node has been used, but in production it is not recommended to use only one node, of course, for safety reasons mentioned earlier in the work.

If the other computer joins this chain, it must also have the installed MultiChain application and must run the command:

```
multichaind BlockchainDiploma@[ip-adress]:[port]
```

After merging other computers/nodes, the first node only has the authority to assign certain rights, such as read and write rights, to other nodes.

Among other things, MultiChain has the ability to store data in a blockchain using the so-called stream. With storage, it also offers the ability to extract data. This functionality is most important for the concept of the application shown here. So, at the main node you need to create a new stream, which we will call certificate/diplomas in this example. The above statement is executed:

```
create stream certificate false
```

The false statement in the command means that only those explicitly licensed addresses can be written in that stream. Since in this example we have only one node that created this stream, it is not necessary to assign special rights. If there is a second node and some other address from which you want to write something on that same stream, you need to assign the rights for each address from the first node by a special grant command.

The next step is to store the data in the created stream certificate/diploma. Data is stored in hexadecimal form. In this example, we will store name and last name and OIBID (personal identification number) with the command `publish certificate key1`

```
476f72616e2046696a61636b6f203638383136393734393035
```

Hexadecimal number

After issuing a command, we can obtain data record from stream using the simple query. The following command gives us all the information recorded in the stream certificate/diploma (Figure 2.4) `liststreamkeys certificate`

2.5.1 Application modules

This type of application is intended for private blockchain. This means that each educational institution should have its own stream that only the people in the

```

gfljacko@gfljacko: ~/Desktop
File Edit View Search Terminal Help
gfljacko@gfljacko:~$ cd Desktop/
gfljacko@gfljacko:~/Desktop$
gfljacko@gfljacko:~/Desktop$ chmod +x installBlockchain.sh
gfljacko@gfljacko:~/Desktop$ ./installBlockchain.sh

MultiChain 1.0.6 Utilities (latest protocol 10011)

Blockchain parameter set was successfully generated.
You can edit it in /home/gfljacko/.multichain/BlockchainDiploma/params.dat before running multichaind for the first time.

To generate blockchain please run "multichaind BlockchainDiploma -daemon".

MultiChain 1.0.6 Daemon (latest protocol 10011)

Starting up node...

Looking for genesis block...
Genesis block found

Other nodes can connect to this node using:
multichaind BlockchainDiploma@192.168.1.121:6819

Listening for API requests on port 6818 (local only - see rpcallowip setting)

Node ready.

MultiChain 1.0.6 RPC client

Interactive mode

BlockchainDiploma: create stream diplome true
{"method": "create", "params": ["stream", "diplome", true], "id": "16081084-1536680626", "chain_name": "BlockchainDiploma"}
9ade58e2aca114237bb5497116bf62678f3712208162e6aef2b736409a029079

```

Figure 2.4: Displaying a textual (CLI) interface where chain creation, chain startup, and creation of a graduate stream are shown.

institution have the authority to store the certificate. All streams are stored in the main book that is distributed to all nodes, that is, educational institutions in this example. The more nodes in the chain, the better, because the chain becomes ever stronger and safer.

The application consists of three modules:

1. Module for certificate/diploma input
2. Certificate/diploma check module
3. Certificate/diploma print module

The first module is for entering a certificate/diploma. It switches the entered data into a hexadecimal form and stores them in the chain and returns the transaction ID (txid) back. Transaction ID is a private key that is awarded to a graduate student because it can be used to check the certificate/diploma data in the chain.

The Certificate/Diploma Check Module, combined with the OIB and Transaction ID, sends a query to the chain and verifies whether there is a record in the chain. Thereafter, it gives a positive or negative answer, depending on whether there is a really required degree in the chain and whether it complies with the OIB entered.

The certificate/diploma printing module prints a certificate/diploma on the screen in PDF format.

All of the modules listed in this example are displayed in the command-line text interface, that is, in the Ubuntu Operating System Terminal. They can also be programmed into a web application and used in WEB browsers.

2.5.2 User roles

Once the student successfully completes the faculty and defends his graduate thesis, the faculty system reports that the student has graduated. With this application and the module for entering the certificate/diploma, an authorized person at the university will enter the name, last name, and OIBID graduate student and this information will be stored in the chain. As a feedback, he receives a Transaction ID, which gives the student and enrolls on the original print certificate/diploma. It can also be printed in the form of a bar code whose scan is the value of the Transaction ID (Figure 2.5).

```

gftjacko@gftjacko: ~/Desktop
File Edit View Search Terminal Help
gftjacko@gftjacko:~/Desktop$ chmod +x diploma.sh
gftjacko@gftjacko:~/Desktop$ ./diploma.sh
1. Unos novog dokumenta
2. Provjera postojanja dokumenta
Odaberite broj [1,2]? 1
Upišite ime i prezime studenta:
Goran Fljačko
Upišite OIB studenta:
68816974905
Diploma uspješno unesena!
Vaš ključ diplome je: 80bbfd9b068259c1f02a72b7196417c5464c54a4b68cfaf6e824777e268ff747

```

Figure 2.5: Certificate input.

The student gets his certificate/diploma and his private key certificate/diploma, which in this case is

80bbfd9b068259c1f02a72b7196417c5464c54a4b68cfaf6e824777e268ff747.

He then reports for a job and after a call from the employer goes to the job interview. The employer asks for a degree to check his qualifications. The procedure is currently being conducted so that the employer contacts the educational institution to verify the validity of the certificate/diploma, most often in writing. This process is long-lasting and consumes a lot of resources. But in this case, the

employer gets a certificate/diploma with a private key. The employer then appoints the OIBID of a person applying for a job and the public key in the application. This way in a fraction of a second returns the information on the validity of the diploma certificate.

After the application's confirmation is answered, the screen prints (Figure 2.6). The name and surname of the student, educational institution, orientation, date and place of graduation are written in the print. The employer eventually has the option of printing a copy of the certificate/diploma for his own archive. If you choose a print option, the certificate/diploma will be generated and opened in PDF format.

For ease of use of the application after release to production, it is a better choice to use it as a WEB application. This means that everything shown will be moved to a web server and the application will access the https protocol (e.g., via URL <https://www.diplome.hr>) in web browsers. This means that users only need an Internet connection and an account in the application to quickly and securely check the validity of the certificate/diploma.

```
Molim Vas odaberite opciju:
1. Unos novog dokumenta
2. Provjera postojanja dokumenta
Odaberite broj [1,2]? 2
OIB:
68816974905
Ključ:
80bbfd9b068259c1f02a72b7196417c5464c54a4b68cfaf6e824777e268ff747
Goran Fijacko diplomirao na Visokom učilištu Algebra, smjer Multimedija, 15.10.2018. u Zagrebu.
Prikazati diplomu?
1. Da
2. Ne
Odaberite broj [1,2]? 1
Diploma će se prikazati u PDF-u!
```

Figure 2.6: Certificate verification module.

2.6 Conclusion

This chapter presents blockchain technology, its history, and the principle of how it functions within the digital identity [15]. In the theoretical part of the chapter, a comparison of the “classical” identity and digital identity is set out, which is described through examples of personal identity cards and e-citizen systems [16]. Then, following the introduction into blockchain technology and describing the method of achieving consensus and transaction logging, the principle of smart contracts is described, which provide the ability to enter code or even complete applications and put them into blockchains, enabling automation of a multitude of processes [17].

This chapter explains common platforms through three examples (Civic, HYPR, Blockverify), and describes business models that use blockchain as a platform for developing their processes based on digital identity. Also, traditional models with those based on smart deals have been compared. Through examples of cancellation or delays in air travel, voting, music industry, and tracking of personal health records, it was established how existing models are actually sluggish, ineffective, and prone to manipulation, and through examples of blockchain implementation, they showed that these systems functioned faster, more transparent, and most importantly, safer.

The middle part of this chapter describes the application of technology in several industries, from the Fintech industry to the insurance and real estate industry. Concepts and test solutions are described, which are slowly implemented in the production phase and show excellent results. For this reason, we believe that similar solutions will be implemented, increasing adoption of blockchain technology globally.

In the last, practical part of the chapter, a survey of existing solutions that offer creation of its own blockchain and a MultiChain platform was selected. For the purpose of this work, it was necessary to create an Ubuntu virtual machine in the Oracle VM VirtualBox, on which we then installed the MultiChain. Through the Ubuntu Terminal, the application concept for entering, issuing, and verifying university certificate/diplomas is presented; and all functionalities and user roles are described in this process.

Motivation for this research came from lack of practical applications of blockchain and importance of EDU certificate transparency and challenges in their sharing (policy issues, national standard, etc.). By having easy to apply and understand guidelines, it is easier for wider audience to accept and use/reuse sometimes complex digital concepts as part of their solutions and business processes. Taking place in novelty approach, we believe this chapter will contribute and be valuable information for future researchers looking to implement blockchain but moreover ones who are looking to improve exchange, storing, and harmonization of often heterogeneous EDU certificates (in forms, acceptability, and content). As part of institutional research lab, explained approach and proof of concept solution was developed in Algebra University College.

References

- [1] Ashworth, Andrew. *Principles of Criminal Law* (5th ed, 2006).
- [2] Avery, Lisa. 'A Return to Life: The Right to Identity and the Right to Identify Argentina's "Living Disappeared"' (2004) 27 *Harvard Women's Law Journal* 235.
- [3] Conte, Frances. 'Sink or Swim Together: Citizenship, Sovereignty, and Free Movement in the European Union and the United States' (2007) 61 *University of Miami Law Review* 331.
- [4] Buergethal, Thomas. 'International Human Rights Law and Institutions: Accomplishments and Prospects' (1988) 63 *Washington Law Review* 1.

- [5] Klepac, G., Kopal, R., & Mršić, L. (2015). Developing Churn Models Using Data Mining Techniques and Social Network Analysis (pp. 1–361). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-6288-9
- [6] Mohr, Richard. 'Identity Crisis: Judgment and the Hollow legal Subject,' 2007 11 Passages – Law, Aesthetics, Politics 106.
- [7] Bromby, Michael., & Ness, Haley. 'Over-observed? What is the Quality of this New Digital World?' Paper presented at 20th Annual Conference of British and Irish Law, Education and Technology Association, Queens University, Belfast, April 2005.
- [8] Nekam, Alexander. The Personality Conception of the Legal Entity (1938).
- [9] Palmer, Stephanie. 'Public, Private and the Human Rights Act 1988: An Ideological Divide'. Cambridge Law Journal, 559, 2007.
- [10] Solove, Daniel. The Digital Person, Technology and Privacy in the Information Age (2004).
- [11] Third, A., Quick K., Bachler M., Domingue J. (2018), Government services and digital identity, Knowledge Media Institute of the Open University.
- [12] Davies, Margaret., & Naffine, Ngaire. Are Persons Property? Legal Debates About Property and Personality (2001).
- [13] UNWTO. UNWTO World Tourism Barometer: Advance Release January 2017. UNWTO. [Online] January 2017.
- [14] World Economic Forum. Digital Transformation Initiative: Aviation, Travel and Tourism Industry. Geneva: World Economic Forum, 2017. REF 060117.
- [15] Derham, David. 'Theories of Legal Personality' in Leicester Webb (ed), Legal Personality and Political Pluralism (1958) 1.
- [16] Naffine, Ngaire. 'Who are Law's Persons? From Cheshire Cats to Responsible Subjects'(2003) May Modern Law Review 346.
- [17] Stacey, Robert. 'A Report on the Erroneous Fingerprint Individualization in the Madrid The Council Of Europe's Convention On Cybercrime. (2001). European Treaty Series 185. Retrieved from http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.