The Proposal of a Blockchain-based Architecture for Transparent Certificate Handling

Jerinas Gresch[1] , Bruno Rodrigues[1] , Eder Scheid[1] , Salil S. Kanhere[2] and Burkhard Stiller[1]

[1] Communication Systems Group (CSG)
Department of Informatics (IfI), University of Zurich (UZH)
jerinas.gresch@uzh.ch, [rodrigues,scheid,stiller]@ifi.uzh.ch
[2] Networked Systems and Security Group (NetSyS)
UNSW Sydney
salil.kanhere@unsw.edu.au

Abstract. Diplomas have high importance in society since they serve as official proofs for education. Therefore, it is not surprising that forgeries of such documents have become commonplace. Thus, employers ordinarily have the diplomas manually verified by the issuer. Blockchain creates opportunities to overcome these obstacles, as it has revolutionized the way in which people interact with each other. Based on this, a holistic solution that includes issuance and verification of diplomas can be realized. This paper presents a proposal of a blockchain based system for managing diplomas called UZHBC (University of ZuricH BlockChain).

Keywords: Blockchain · Education · Diploma · Verification · Digitalization

1 Introduction

In an increasingly competitive market, a diploma from a higher education institution has a major relevance in the labor market. Diplomas are seen as a sign of capability, certifying the level of education and skills of individuals. Globally, enterprises are having difficulties in finding skilled professionals to fill up vacancies [17]. Unfortunately, this has led to an increase in *diploma fraud* which ranges from inflating academic grades to outright fake diplomas. There now exist several 'diploma mills', *i.e.,* unscrupulous organizations with the sole purpose of providing illegitimate academic degrees and diplomas. The number of individuals owning fake credentials globally is hard to estimate. In 2015 the Association of Certified Fraud Examiners [13] estimated that only in US (United States) about 41% of job applicants presented falsified information about their education. In 2017, it is estimated that about 500 fake doctoral diplomas are sold monthly in the US [14].

Recognition and accreditation systems are commonly used to verify which institutions are recognized (*i.e.,* trusted or reputable) and authorized to award

Algorithm 1: Mechanism to issue files as hashes to a Smart Contract

```
Input: diploma_Files⟵PDF files that are created by the UZH
Output: Success message from the Smart Contract
begin
    hash_List ← filesToSHA3(diploma_Files)
    batch_Size ← calculateBatchSize(hash_List)
    num_Of_Batch ← hash_List.size() / batch_Size
    for each batch ∈ num_Of_Batch:
        tmp_Batch ←
          slizeToBatch(hash_List, batch · batch_Size, (batch + 1) · batch_Size)
        unlock_Account(password)
        if account.status == unlocked:
            transaction_msg ←
              web3.UZH_Contract.sendTransaction(owner, tmpBatch)
            if transaction_msg == success:
                msg = transaction_completed
            else:
                msg = transaction_rejected
```

academic or professional qualifications. However, this system is not always effective in countries where the recognized higher education institutions cannot meet the demand of certified professionals required by the labor market. This creates a fertile ground for these 'diploma mills' to sell fake credentials to unqualified individuals attempting to take advantage of this shortfall. In this regard, the digitalization of the processes of issuing and verifying diplomas including cryptography primitives to ensure the identity of the diplomas becomes increasingly important to ensure that enterprises are recruiting truly qualified individuals.

Currently, the majority of diplomas is granted in a paper-based format, which can easily be faked and scanned into a digital representation. As a countermeasure, many universities implement mechanisms [20] or use services [6] to issue and verify a digital representation of the paper-based diploma. The verification can be automated by including the identity of the diploma into a central database, which can be accessed by a company wishing to verify the credentials. However, this process is rather ad-hoc and there are no unified mechanisms or standards in place such as a public registry, that is maintained by multiple institutions and accessible for everyone.

As mentioned in [8, 21], there is not a perfect type of diploma certification. While paper-based diplomas are still seen as the cheaper and safest form of accreditation, it has some drawbacks in contrast to digital-based diplomas. For example, paper-based diplomas require more manual tasks for issuing and verifying diplomas than a digital one, and the security of these diplomas are as high as the level and expertise that one has to include security features such as watermarks or invisible fibers. In contrast, digital diplomas are more simple to

be issued and verified against a central database maintaining these diplomas, and their security relies on available security cryptographic protocols.

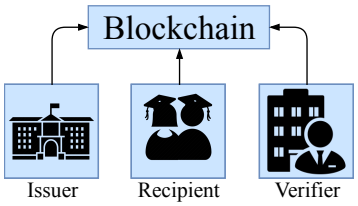

Fig. 1: Stakeholders

Digital diplomas using a centralized database, however, have some drawbacks that blockchain-based approach can overcome. For example, centralized databases are a single point of failure and using a blockchain (*c.f.,* Figure 1), issued diplomas cannot be tampered with as data stored in a block is replicated across the blockchain network. Once blocks are distributed, any party connected to the blockchain can access the stored diplomas, meaning that any verifier in possession of a diploma can easily verify the authenticity of the diploma. Furthermore, hashes can create a link between the original paper-based diploma which is held by the recipient to a verifier, which can then check whether the hash stored by the issuer represents the original diploma.

Recently, there have been works ([2, 4, 5]) on the use of blockchain technology for creating a standardized platform for issuing and verifying diplomas. Thus, the infrastructure maintaining the information related to the diplomas is transparently replicated by the chain of nodes, so that it is not possible to change diplomas issued by previously authorized institutions. This way, only diplomas created by valid issuers are published and the falsification of diplomas can be omitted. Based on these works, a blockchain based end to end system is presented in this paper, implementing an approach to issue and verify diplomas at the Univerisity of Zurich (UZH).

This paper is structured as follows: In the next section, known projects related to this approach will be discussed. Thereupon the identified requirements as well as the structure of the prototype are presented. In section 4, a preliminary evaluation that illustrates how the proposed framework meets the requirements is shown. The paper ends with a final consideration.

2 Related Work

When blockchain is used for the issuance of diplomas, there is an opportunity not just to verify a degree certificate, but to enrich and add value to the verification ecosystem. In its purest form, a blockchain acts like a shared, replicated, append-only database where participants can depending share, write, access and

participate in the validation process [3, 16]. By providing a trustworthy, decentralized, and publicly available data storage, blockchain has become a disruptive technology that has seen interest from many application domains beyond FinTech (Financial Technology) area. Although the application of blockchains in education is in its infancy, there are many interesting projects (blockchain-based or not) that have explored the possibility of digital diplomas as a countermeasure to fake diplomas.

BADGR [1] and Mozilla Open Badges [12], both present unified solutions for managing the entire educational history of students by collating all digital certifications acquired by them at different academic institutes and associating it with a single identity. Although these solutions do not use blockchain, they demonstrate how to integrate multiple certifications into a student identity.

The goal of blockchain in the educational area is to create a digital certificate into an automatically verifiable piece of information that can be consulted by third parties through an immutable proof system. According to [8], blockchain can be implemented in two distinct ways in the area of education. While the first requires that diplomas be stored in plain text to create a publicly available database, the second requires that only the hash of a diploma be stored to secure the digital certificate awarded to the student. Therefore, published student data can be seen by anyone, as they are not containing any confidential information. As the diplomas are required to be tamper-proof, using a blockchain as a decentralized storage is appropriate.

The first notable use case storing a hash of diplomas is Blockcerts [11], an initiative by the MIT (Massachusetts Institute of Technology) to create an open standard for issuing and verifying credentials on the Bitcoin blockchain. The stored diplomas are accessible via an App termed Blockerts wallet, which enables students to get a verifiable, tamper-proof version of their diploma which they can share with employers, schools, family, and friends. Blockcert is seen as an enabler towards digital certificates in the blockchain.

Similar to the approach of Blockcerts, the National Research and Education Network of Greece (GRNET) [4] are also storing the hashes of diplomas in a blockchain in order to protect the confidential student data. The goal is to create a system that can verify student diplomas on the Cardano blockchain reducing the manual verification process and cases of fake diplomas. However, the GRNET project [4] differs from Blockcerts [11] in the sense that it can store not only hashes of diplomas, but also the entire verification process. Verification requests, successful or unsuccessful proof and the forwarding of the result to its requester are steps that will be stored.

BCDiploma [2], EduCTX [18] and UNIC (University of Nicosia) [19] have started their blockchain-based projects to issue and verify diplomas. BCDiploma and EduCTX share the same goal towards a global certification network of higher academic institutions. However, UNIC aims to digitize and decentralize their internal processes having issued their first academic certificates as a proof of concept. Although these approaches are already mature, they either are not meeting the requirements of the UZH or are not easy to integrate into the structure of

a university. Therefore, this work shows a prototype that, besides considering these works as starting points, taking into account specific requirements raised from the UZH. For instance, the ease of deployment into their existing IT infrastructure, extending the existing functionality to create diplomas.

To guarantee the authenticity of a document, digital signatures can also be used. However, the UZH stated not to apply this solution, mainly because of cost reasons. Also, software exists that can bypass those protections and manipulate the content of a document [22].

3 System Overview

This Section discusses key requirements for such a system (*c.f.,* Section 3.1). Further, it is presented the development of the prototype based on the architecture design and the performed implementation are detailed (*c.f.,* respectively, Sections 3.2 and 3.3).

3.1 UZH Requirements

Table 1 presents the requirements derived from interviews with stakeholders. This includes the student administration office, that is responsible for the verification. Also, the faculty of economic science, which issues the diplomas for all economic students, was questioned. To not violate any legal aspects, the data privacy protection department of the UZH was interviewed. For all IT relevant topics, the UZH employs the *Zentrale Informatik*[3] (ZI), who provides IT infrastructure, software and services for students and employees of the UZH (herein termed legacy system). While, RQ (Requirements) 1-4 are related to the issuer, *i.e.,* conditions that UZH demands from the system, RQ5-6 are related with the requirements for a company that wants to verify diplomas. The most named requesters of verifications by the student administration office were background check companies. Finally, RQ7 is related to the delivery of the diploma in a digital form to the student.

- **RQ1**: related to the guarantee that diplomas can only be issued by authorized issuing instances, for example, UZH faculties. Thus, diploma mills are not able to fabricate any certificates. For the verifiers, it is important to be ensured that the diplomas can only be issued by the university.
- **RQ2**: addresses the confidentiality of student data, which should only be accessible by the student and potential verifiers. Also, the 'right to be forgotten' defined in the new GDPR (General Data Protection Regulation) declares that data of consumer (*i.e.,* students) cannot be permanently stored [15]. Hence, the diploma itself cannot be stored in the blockchain. The blockchain should therefore store a hash of the document in order to prove the authenticity of the digital diploma sent to the student.

[3] Zentrale Informatik: http://www.id.uzh.ch/de.html

Table 1: Requirements elicited during Interviews with Stakeholders

Issuer	
RQ1	Only authorized UZH departments are allowed to issue diplomas
RQ2	Diploma data should be confidential to its recipients
RQ3	Process of issuing and verifying diplomas should abstract technical complexities
RQ4	Multiple diplomas should be processable in batch
Verifier	
RQ5	Verification capabilities should be accessible to any company
RQ6	Diplomas should be verified autonomously
Recipient	
RQ7	Graduates should receive their diplomas in a digital format

- **RQ3**: defines that technical details involved in the process of issuing diplomas must remain transparent to involved users (issuers, verifiers and recipients). In this sense, the use of blockchain (or any other infrastructure) for issuing or verifying diplomas should not require technical know-how from the users (*e.g.,* extracting the hash of a diploma at the verification process).
- **RQ4**: relates to the system scalability concerning the ease to create and verify multiple diplomas at once, as in a bash service. The goal is to avoid manual exchange of information between companies wishing to verify diplomas and the university as an issuer instance.
- **RQ5**: allows anyone in possession of a diploma hash to verify its authenticity. As any company that receives a diploma from a graduate might want to verify its authenticity, this functionality has to be publicly accessible.
- **RQ6**: describes an always available service with an automated response of the verification. If the diploma is authentic, the system has to recognize it, whereas tampered documents need to be rejected
- **RQ7**: graduates shall receive their diplomas in a digital format. Physical diplomas can get lost or damaged, whereas digital diplomas are not affected by these problems. In addition, forgery of physical documents is generally easier.

3.2 Design

Overall, the system (*c.f.,* Figure 2) is divided in three different parts. The first covers issuer requirements and the second covers recipient (graduate student) requirements. The third is related to companies wishing to verify a diploma sent by recipients. At the UZH side, the issuing instance, the system is embedded into the legacy system, taking as input diplomas in a digital form (.PDF files). Currently, these digital diplomas are not sent to students but used to print paper-based diplomas which are then granted to graduate students.

In the first step, the issuing institution has to create the digital diploma, which is part of UZH legacy system workflow. Currently, the generated digital diploma (PDF document) is used only for printing the paper-based diploma and

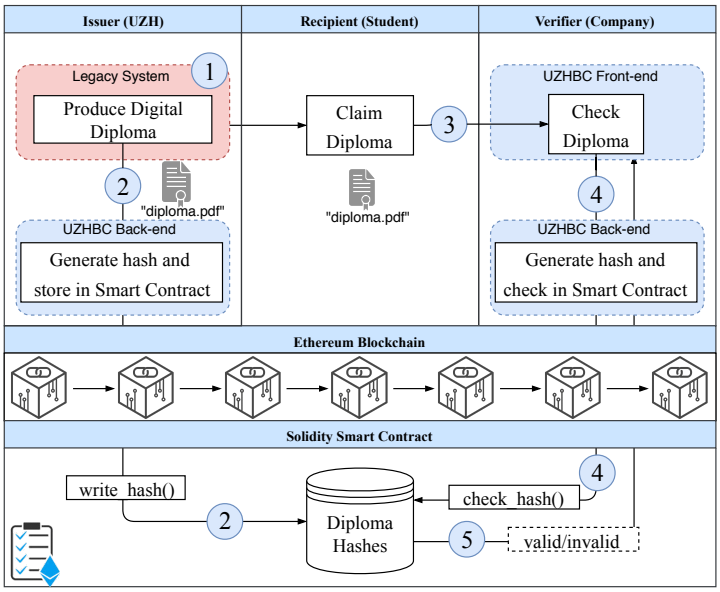

Fig. 2: UZHBC System Architecture.

it is not made available to the recipient. In a second step, the UZHBC back-end requires this PDF document as input to generate an one-way hash function corresponding to the paper-based diploma. This hash will be stored in a smart contract, that is deployed on the Ethereum blockchain. A verifier company that receives the diploma from a student could then verify the authenticity of the document without contacting the university. Therefore, the verifier can use the UZHBC front-end, that takes the digital diploma as an input to check the authenticity of the hash. This hash will be compared with all hashes that are contained in the smart contract. If it exists, the verification will return successfully and informs the company that the diploma is authentic. If no match occurs, the system also gives a feedback.

3.3 Implementation Details

3.3.1. Front-End The user can interact with the system through an HTML5 and JavaScript-based web page. To cover the two functionalities, issuing and verifying, two input fields are provided. These inputs expect documents from the type PDF and are meant to insert the diplomas. The calculated hash of the documents will also be displayed. Also, a password field is provided, which is needed to regulate the writing access into the blockchain. The screens to issue and verify are depicted in Figure 3 and Figure 4.

Fig. 3: Front-end interface to issue diplomas

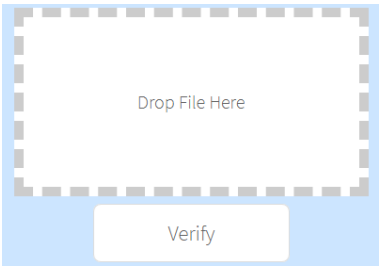

Fig. 4: Front-end interface to verify diplomas

3.3.2. Back-end The back-end has the functions to take the documents from the input fields, convert them to hashes and send them to the smart contract. The hashes are calculated with the SHA-3 checksum, which takes any kind of data as input and returns a hash with the size of 256 bits [10]. To interact with the Smart Contract deployed on the Ethereum blockchain, the web3.js-Library is used [7]. Also, the associated owner of the smart contract is used as a standard account to send transactions and requires a password. Also, Web3 handles the connection between client and *Geth*. *Geth* is the official Ethereum client and is responsible for creating the local copy of the Ethereum's network state. *Geth* must be syncing in the background to run this application and needs to be attached to *localhost:8545* in order to communicate with web3 client.

3.3.3. Smart Contract The smart contract contains only two functions. The write function `issueCertificate` is responsible to store the hashes into the smart contract. Also, it is only possible to call this function as an owner of the contract, which is the university. The dedicated code is depicted in listing 1.1.

```
1  function issueCertificate(string _diplomaHash) public {
2      if (msg.sender != owner)
3            revert();
4      diplomaHashes.push(_diplomaHash);
5  }
```

Listing 1.1: Function to write a hash in the smart contract

```
function verifyCertificate(string diplomaHash_) public
    constant returns (bool) {
  uint counter = 0;
  bool verified = false;
  while(counter<diplomaHashes.length){
      if(keccak256(diplomaHashes[counter])==keccak256(
          diplomaHash_)){
          verified = true;
          return verified;
      }else{
          counter++;
              }
  }
  return verified;
}
```

Listing 1.2: Function to check if the smart contract contains a hash

The hashes are stored in an array of strings. When a verification request occurs, the `verifyCertificate` method will iterate through the array of hashes. If any hash in the array matches with the given hash from the parameter, the method returns `true` as an indicator of a verified diploma. At the moment, Solidity, the underlying programing language of smart contracts, does not provide functionalities to compare strings. Therefore, the function `keccak256()` is used to hash the strings which allows to make them comparable again. The dedicated code is depicted in listing 1.2. Since this is a prototype, the Smart Contract is deployed on the Rinkeby testnet of the Ethereum blockchain.

4 Preliminary Evaluation

This Section discusses the preliminary evaluation of the UZHBC prototype. An analysis is conducted to verify whether the prototype can satisfy the requirements identified in Section 2. Likewise, the fulfillment of the requirements by the related work was analyzed and compared against the prototype. This comparison is presented in Table 2.

The UZH consists of seven faculties whereas each faculty includes many departments. In UZHBC, each of these faculties would represent an issuing instance able to record diploma hashes into the blockchain. Other blockchain-based approaches such as Blockcerts [11] and BCDiploma [2] extended the number of issuers in their works. For example, new issuing institutions can register itself on the platform which could work as a universal diploma verifier. However, at some point, new issuers would have to prove their ability to certify diplomas to the developers of the platform. This dependency between developers and issuers cannot be neglected, and a fully automated process cannot be achieved. The most critical issue is that this prototype is intended to solve the falsification of diplomas through individuals or diploma mills. Therefore, granting issuing rights needs to be strictly regulated and the ability to add issuers is not desired.

Table 2: Related Work on Requirements

	Blockcerts	GRNET	EduCTX	UNIC	BCDiploma	BADGR	UZHBC
RQ1	✗	✓*	✓*	✓	✗	✗	✓
RQ2	✓	✓	✗	✓	✓*	✗	✓
RQ3	✗	✗	✗	✗	✗	✗	✓
RQ4	✓	✓	✗	✓	✓	✗	✓
RQ5	✓*	✓*	✓*	✓	✓	✓	✓
RQ6	✓	✓	✓	✓	✓	✓	✓
RQ7	✓	✓	✓	✓	✓	✓	✓

Note: * indicates that the requirements has been partially met.

However, it is important to note that the different UZH faculties are acting independently. The requirements to graduate, deadlines to be met, and the entire process of graduating are different at each faculty. Thus, a faculty has to be considered as an autonomous entity with respect to the issuance of diplomas.

The provided UZHBC functionalities achieve the requirement (RQ1) as presented in listing 1.2, which shows that writing access is only granted to the actual owner of the smart contract, the UZH. Similar to Blockcerts and BCdiploma, GRNET [4] and EduCTX [] allow multiple issuers. Nevertheless, write permissions are not readily granted. While GRNET consists of a group of predefined universities as issuers, new universities at UniCTX should be selected by the existing participants.

Regarding the RQ2, a hash generated through a one-way function is used to represent the diploma. By only recording the hash, one is not possible to identify confidential data about the actual content of the diploma. To verify the authenticity of a diploma, a verifier needs an actual diploma document sent by a student (*e.g.*, in a job application). The provided functionality for verification generates a hash again, and if this hash is already contained in the smart contract, it can be considered as authentic. Issued hashes are publicly available without compromising the confidentiality of its owner.

As depicted in Table 2) many approaches also use cryptographic hashes. BCDiploma [2] store encrypted diploma data and claims to solve the problem of the new GDPR "right to be forgotten" [15]. Diplomas can be decrypted through a persistence key, which is unique and kept by the owner of the diploma. However, losing this key implies that the diploma cannot be retrieved anymore and encrypted data would remain on the blockchain.

Intensive acceptance and usability test scores with the university and verifiers are required to gain more insights concerning system practicability. However, the amount of interaction with the system, which can be seen as the actual additional effort, require fewer interactions in contrast to other approaches. This includes sending invitations or transaction addresses, registration, maintaining a hash list, etc. Therefore, it must be stated that comparing different approaches is not straightforward since these are slightly different concerning their function-

alities. As UZHBC currently offers two interaction possibilities (recording and verifying), complexity is reduced to a minimum (RQ3). For example, these functionalities are translated into a simple action at the front-end, such as dragging a file into a field.

The UZHBC can verify the authenticity of diplomas without relying on manual intervention by the university. However, it requires some additional steps to achieve this. At the point where the paper-based diplomas are delivered to graduates, the digital equivalents have to be processed into the system. The extra effort can be limited since the prototype allows to prepare as many documents as desired. As the UZH handle diplomas in batches (for printing), it is also feasible to use the prototype and RQ4 can be met.

As confidential data is not disclosed in the verification process, the front-end interface can be publicly accessible (RQ5). Other approaches (*e.g.,* Blockcerts [11] and EduCTX [18]) uses invitation mechanisms, where the graduates sends a link to his academic credentials. With UZHBC (and UNIC [19]), this invitation is handled by sending the digital diploma in a job application. The interface of verification is accessible to everyone, but without a diploma, it is useless. It is important that awareness of such a system needs to be spread, so employers know where to verify the received diplomas.

Background-check companies, headhunters and also regular companies are the typical entities that need to verify student diplomas. This task is currently seen as rather time-consuming as there is no automated verification system for diplomas currently in Switzerland. Thus, the process relies on the manual interaction between the employer, university, and graduate. Nonetheless, universities in Switzerland are not allowed to send any information without the consent of the graduate. Thus, verification requests are rather time-consuming. Based on UZHBC, verifiers are only required to send the received digital diploma to the front-end verification provided UZH. Therefore, the hash will be generated again and checked at the blockchain whether it is authentic or not, fulfilling the initial requirement from the employers (RQ6).

From the perspective of the recipients, *i.e.,* graduate students, digital diplomas would be granted in addition to the conventional paper-based diplomas [9]. At the moment, these are obtained by scanning the paper-based document to have a digital equivalent. To fulfill RQ7, the UZH will deliver, through the UZHBC system, these documents added to the paper-based diplomas. However, this requirement relies on the cooperation of the university concerning its internal regimentations. This is also a prerequisite for the other related work, as all the academic credentials are handled digitally.

5 Final Considerations

The digitalization of the processes within the UZH for issuing and verifying diplomas including cryptography primitives to ensure the identity of the diplomas becomes an increasing necessity. In this paper, it was presented a prototype tailored to the UZH needs to record and verify diplomas issued by its faculties.

The first step was to determine the requirements of the university's stakeholders to create an initial prototype which demonstrates the functionalities and highlight advantages. Subsequently, other improvements are foreseen as future work. For instance, as the project started as a research initiative by the authors in contact with the technical UZH department, the UZH board of directors also need to approve the project. Then, the system should include adaptations fully comply with the university's internal regulations. Also, further universities or colleges should be included as issuers in Switzerland. As the UZH is not the only institution that has to deal with diploma fraud, verification is a general concern.

References

1. Badgr.io: Make your badges meaningful with Badgr (May 2018), https://info.badgr.io
2. BCDiploma: Degrees Certified on the Blockchain (August 2017), https://bit.ly/2rp95qC
3. Bocek, T., Stiller, B.: Smart contracts–blockchains in the wings. In: Digital Marketplaces Unleashed, pp. 169–184. Springer (2018)
4. Castor, A.: Cardano Blockchain's First Use Case: Proof of University Diplomas in Greece (January 2018), https://bit.ly/2DVsrYt
5. Elizabeth Durant, A.T.: Digital Diploma debuts at MIT (Oct 2017), https://bit.ly/2xPRWXC
6. eQuals, M.: The Official Platform of Australian and New Zealand Universities (Jan 2017), https://bit.ly/2qjHtE9
7. Ethereum: Ethereum JavaScript API (Feb 2015), https://github.com/ethereum/web3.js
8. Grech, A., Camilleri, A.F.: Blockchain in Education. Tech. rep. (2017)
9. Jerinas, G.: Survey about digital academic certificates (May 2018), https://bit.ly/2wLFXyP
10. Mattias Andre: SHA-3 and Keccak checksum utility (Nov 2017), https://github.com/maandree/sha3sum
11. MIT Registrar's Office: Digital diploma pilot program faqs (Sept 2017), https://bit.ly/2JYw4zT
12. Mozilla: Open Badges (May 2018), https://openbadges.org/
13. Musee, N.M.: An Academic Certification Verification System Based on Cloud Computing Environment. PhD diss., University of Nairobi (2015)
14. Park, H., Craddock, A.: Diploma Mills: 9 Strategies for Tackling One of Higher Educations Most Wicked Problems (Dec 2017), https://bit.ly/2DoEeyu
15. Regulation, G.D.P.: Right to erasure (right to be forgotten) (May 2018), https://bit.ly/2zMT9Vl
16. Rodrigues, B., Bocek, T., Stiller, B.: The use of blockchains: Application-driven analysis of applicability. In: Pethuru Raj, G.D. (ed.) Blockchain Technology: Platforms, Tools and Use Cases, Advances in Computers, vol. 111, pp. – . Elsevier (2018). https://doi.org/https://doi.org/10.1016/bs.adcom.2018.03.011, https://www.sciencedirect.com/science/article/pii/S006524581830024X
17. Rutkowski, J.: From the shortage of jobs to the shortage of skilled workers: labor markets in the eu new member states (2007)
18. Turkanović, M., Hölbl, M., Košič, K., Heričko, M., Kamišalić, A.: EduCTX: A Blockchain-based Higher Education Credit Platform. IEEE Access (2018)
19. University of Nicosia: Academic Certificates on the Blockchain (Mar 2018), https://bit.ly/2I5G3mj
20. USD: University of South Denmark. The Digital Diploma (Jan 2018), https://bit.ly/2I3Bid5
21. Warasart, M., Kuacharoen, P.: Paper-based Document Authentication using Digital Signature and QR Code. International Conference on Computer Engineering and Technology (ICCET 2012) (April 2012)
22. Zeichick, A.: Can Blockchain Solve Your Document And Digital Signature Headaches? (Apr 2018), https://bit.ly/2tstjkx