# A Technology-driven Overview on Blockchain-based Academic Certificate Handling

Bruno Rodrigues, Muriel Franco, Eder Scheid, Burkhard Stiller and Salil S. Kanhere*

*CSG@IfI, University of Zürich, Binzmühlestr. 14, 8050 Zürich, Switzerland*

**Networked Systems and Security Group NetSyS, UNSW Sydney, NSW 2052 Australia*

*[rodrigues¦franco ¦sheid¦stiller]@ifi.uzh.ch*

*salil.kanhere@unsw.edu.au*

## Abstract

Academic certificates have a significant influence on the job market, proving a particular competence or skill of a recipient. However, the ability to verify the authenticity of certificates does not follow its relevance in the labor market, causing several companies to exploit this inefficiency to falsify information or even to make fake certificates. In this context, several proposals based on blockchain appear as a technological alternative to increase the transparency and the ease of verification of these certificates. This chapter discusses the main proposals toward the handling of academic certificates from a technological point of view, discussing the technical aspects that may influence the relationship between confidentiality and transparency as well as application requirements such as performance and reliability in contrast to the blockchain characteristics. Finally, this chapter summarizes the key challenges and opportunities based on this discussion outlining future directions for academic certificate management.

Keywords: Blockchain, Technology, Education, Certificates, Diploma, Recognition, Accreditation, Distributed Systems

## 1 Introduction and Motivation

Academic certificates are seen as a proof of capability certifying the level of education and skills of individuals. With an increasingly competitive labor market and employers with large applicant pools, it is a necessity to require a certain level of education for crucial positions. While applicants tend to “exaggerate” or even just fake certificates about their educational history to make it more desirable to the employer, job recruiters are usually overwhelmed with applications which makes it difficult to verify all certificates described by all applicants. In some cases, applicants even purchase fake diplomas from so-called *diploma mills* to declare that one has completed a program of postsecondary education or a specific technical training.

The extension of these fraudulent activities can be observed in numbers as reported by The World Education Services (Hanna Park, 2017), which estimated, in the year of 2017, that there are around 2’615 active *diploma mills* in the world. From these active *diploma mills*, almost half (1’008) operate only in the United States (US). These numbers reinforce the research conducted two years before by the Association of Certified Fraud Examiners (ACFE) (Nicholas Musee, 2015), which estimated that 41%

of job applicants in the US presented some type of falsified information about their education. As of today, educational experts (Jeremy Alder, 2017) estimates that about 500 fake Ph.D. degrees are sold monthly in the US, creating a parallel market of around 200 million US dollars of revenue.

According to (Grech and Camilleri, 2017; Merija and Kapenieks, 2018; Breuls et al., 2018), the increase in these numbers occurs mainly because of the following factors:

- The increasing number of non-accredited educational institutions seeking to meet the demand for higher degree diplomas, and the lack of governmental measures to ensure the quality of these institutions. While some countries implement quality assurance procedures for their higher education institutions, other countries lack the same effective measures enabling transnational companies to exploit this lack of quality control in certain countries to issue diplomas.
- The inability of traditional, paper-based, certification systems to allow an agile and effective verification of issued diplomas. Also, such form of certificates and diplomas issued on paper are relatively easy to counterfeit and rely on the ineffectiveness of processes to verify their authenticity.

The current system based on data (*e.g.,* certificates, diplomas, and documents) privately stored in databases of each educational institution transforms a simple verification process in a complicated, cumbersome, and expensive process. If an employer wants to verify the authenticity of a certificate, it is not only necessary to interview the applicant to check whether the skills informed in its Curriculum Vitae (CV) are trustful, but also to contact a recognition or accreditation system to verify whether the diploma or certificate claimed were issued by a recognized institution authorized to award academic or professional qualifications.

Third-party recognition and accreditation systems are commonly used to check whether institutions are recognized (*i.e.,* trusted or reputable) (Gresch et al., 2018). However, these systems are not always effective in countries where higher education institutions cannot meet the demand for certified professionals required by the labor market. Overall, this leads to an increase in diploma frauds, which ranges from inflating academic grades to outright fake diplomas. Due to the massive process of verifying each unstructured information presented by a large number of candidates, there is a tendency that the verification process, which is also typically performed manually, is prone to errors. From a technological point of view, a common practice of human resources companies is to build their databases gathering applicant's information (*e.g.,* skills, performance ratings, age, educational background) to better understand company's requirement, performance, and talent acquisition (Angrave et al., 2016).

Despite the use of big data tools to analyze data from job applicants and the fact that these provide a more accurate view or prediction regarding a company's human resources, the output of the analysis is useless when it is mostly based on falsified data. As pointed in (Scholz, 2017), despite facilitating the work of employers by connecting possible problems with possible solutions through successive algorithmic analyzes, big data does not solve the problem of verifying falsified data presented by candidates. Moreover, big data analytics are not accurate when the database in which they operate is not really "big," as described in (Scholz, 2017). Therefore, the fact that companies maintain human resources information centralized in their databases makes the accurate analysis of these algorithms directly linked to the size of their database.

An effective solution to verify the authenticity of the information provided by applicants is to rely on digital signatures (Warasart and Kuacharoen, 2012), which represents a digital fingerprint of the owner in a digital or even paper-based version of the document. This digital signature is typically generated based on cryptographic hash functions and asymmetric cryptography, which relies on a signature of the owner with its private key to produce a unique signature of the document that can be verified with the public key of the owner. However, the major issue of the employment of digital signatures into daily life is that it is not always possible to eliminate the existence of paper-based documents. Also, although it is possible to produce academic certificates in both digital and paper-based form, the problem of centralization of information persists.

In this sense, the blockchain technology provides a trustworthy, decentralized, and publicly available data storage (Grech and Camilleri, 2017). The immutability is one of the essential attributes of this novel technology, which brings many benefits to many applications that demand non-repudiation features to avoid forging data. Once transactions are written in a block, distributed over the blockchain network, and chained with other blocks, it is not possible to forge the respective transactions on the entire blockchain network. Therefore, the combination of strategies for digital verification and validation of documents with blockchain can be an ideal solution to combat the increase of fraudulent activities in this context.

The process of issuing diplomas and certificates can be done in the blockchain (Merija and Kapenieks, 2018), for example, to guarantee the authenticity of this document without the need for a long internal validation process (Grech and Camilleri, 2017; Gresch et al. 2018). Thus, anyone connected to the blockchain may access the diplomas, meaning that application verifiers can quickly check the authenticity of the diploma. Furthermore, a fingerprint of the original document stored in the blockchain can create a link between the original paper-based or electronic copy of the diploma, which is held by the recipient to a verifier, who can then check whether this fingerprint stored by the issuer represents the original document.

Recently, there have been several proposals from academia and industry seeking to explore the use of technology for the emission and validation of diplomas. The goal of this Chapter is to describe and evaluate these proposals from a technological perspective, discussing their advantages and drawbacks as well as applicability and user requirements for the issuance of diplomas. Based on this discussion, the Chapter points out future directions of research, not only in the technological but also within the political and organizational field, which may prevent the widespread use of blockchain in the process of issuing and validating diplomas.

In this sense, the Chapter analyzes the state-of-the-art extensively, categorizing approaches not only according to the dedicated blockchain technologies on which they are based on but also in the way in which the technology was exploited. With this, the reader is expected to gain a broad view of the subject and to understand the state-of-the-art and different ways the blockchain technology is used to solve the problem of verifying diplomas and certificates reliably in a decentralized manner.

This Chapter is structured as follows. Section 1 introduces the need to digitize and decentralize the validation of certificates in education, as well as how the blockchain technology can help to address these issues. Section 2 has as objective the theoretical foundation about the technological details and different ways in which blockchain can be used, mapping these to the problem. Section 3 has as objective the description of the related works, categorizing them according to the characteristics raised in Section 2 and grouping them according to their focus within the area of education. Section 4 shall discuss these works by presenting a table which summarizes the description of Section 3. Finally, Section 5 concludes the Chapter by presenting final remarks and future directions for research.

## 2 Blockchain in Education

In its purest form, *i.e.,* as proposed in Bitcoin (Nakamoto, 2008), a blockchain acts as a decentralized and public digital ledger that transparently and permanently record blocks of transactions across computers based on a consensus algorithm without modifying the subsequent blocks. However, permissions to write and read as well as the participation in the block-validation process can be distributed in different ways in a blockchain (Rodrigues et al. 2018). A blockchain can be permissionless (*i.e.,* public) where all participants can read and write transactions or permissioned (*e.g.,* fully private or in a consortium-based approach). In these different deployment scenarios, different consensus algorithms (*e.g.,* Proof-of-Work - PoW, Proof-of-Stake - PoS) can be used to ensure that all nodes maintain the same, updated view over the chain, and prevent issues such as double spending.

Considering the academic certificate handling involving the creation (issuance) and verification, blockchain features are especially advantageous in contrast to traditional digital certification systems, such as digital signatures. The main advantage stems from its disintermediation power, which reduces the need of trust in a specific third-party. However, there are different trade-offs to be observed in its characteristic as there is always a need to trust that the issuing certificates are accredited. If on the one hand blockchain can act as a public and distributed ledger of academic certificates, on the other hand it is necessary to trust the institutions that are issuing certificates in this ledger, which revolves to the question of trust. It is important to observe, however, that existing systems still requires trust in the entities issuing certificates, additionally making the verification process difficult as these academic certificates are typically stored in private databases.

Although the blockchain does not provide a completely trustless solution, the inherent disintermediation contributes through its transparency to an increase of trust among the stakeholders involved. For example, with greater transparency among students, academia, and industry, the processes of issuing and verifying certificates is more reliable. Consequently, it is necessary that the academic institutions issuing certificates be duly accredited and recognized, as with existing accreditation systems. Therefore, it is imperative that this blockchain restricts writing only to selected or accredited academic institutions, making it a permissioned database. However, the reading must be public in a way that any industry entity is able to verify a claimed certificate by a student whose certificate was issued by one of the institutions.

While blockchain was originally proposed in Bitcoin as a completely public platform, *i.e.,* anyone can submit transactions, participate in the consensus process, and read the transaction history, there are different types of blockchain in which these characteristics can be modified (*cf*. Figure 1). These different types are categorized as follows (Rodrigues et al. 2018; Karl and Gervais, 2017):

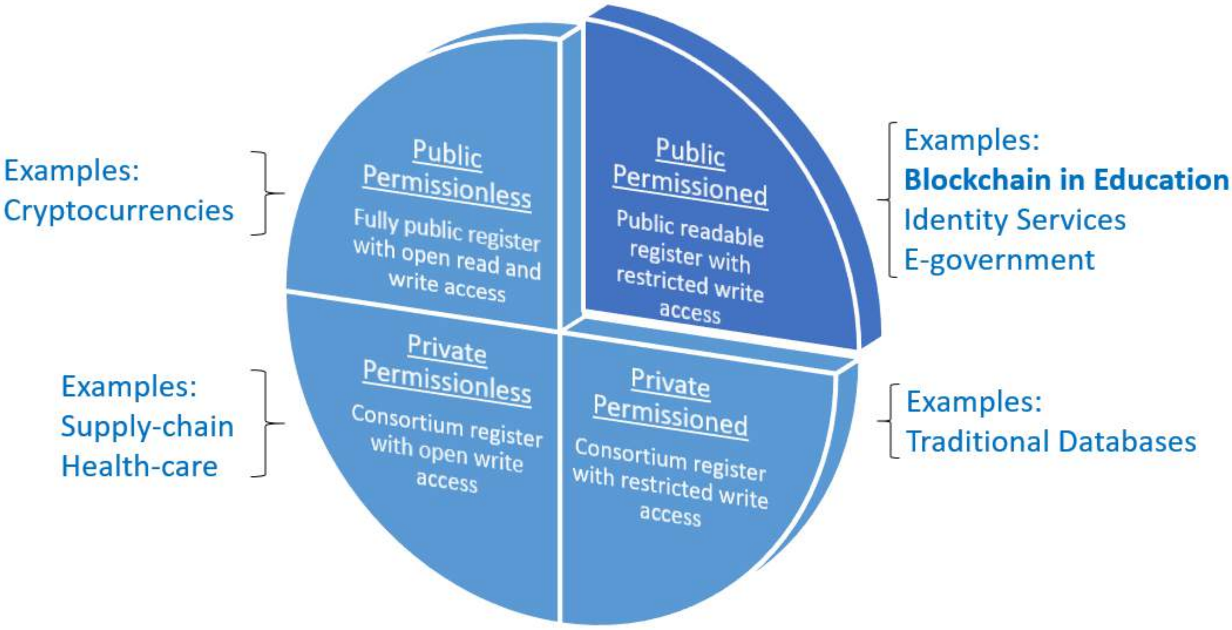


Figure 1 - Blockchain Deployment Types

- **Public Permissionless**: write and reading permissions, as well as the participation in the consensus, are open to anyone with Internet access. This is the most traditional blockchain deployment case as observed in most cryptocurrencies.

- **Public Permissioned**: writing permissions are restricted to selected entities, but writing permissions remain open to anyone accessing the Internet. For example, it is the case of applications whose writing authorities are trusted, and the result of their writing requires public verification (*e.g.,* handling academic certificates).

- **Private Permissionless**: works similarly to the public permissionless, but the notion of "public" is restricted to a certain group or community. Therefore, the writing and reading permissions are open to all participating members of this Private blockchain. As examples, one could consider a supply chain which the exchanged information only concerns its members.

- **Private Permissioned**: is the case in which the use of blockchain becomes questionable since this is typically the case for traditional databases. In a private permissioned deployment write and read permissions are restricted, creating a hierarchy between its participants (*e.g.* role-based actions) where the main features of blockchain (*e.g.*, transparency, immutability, decentralization) may not make sense for a potential application.

The relationship among stakeholders based on a published and permissioned blockchain is illustrated in Figure 2. There are one or more *Issuers*, which are educational institutions responsible for certifying that one or more *Recipients* have a certain skill, as well as one or more *Verifiers* that desires to certify whether one or more recipients have the claimed certificate.

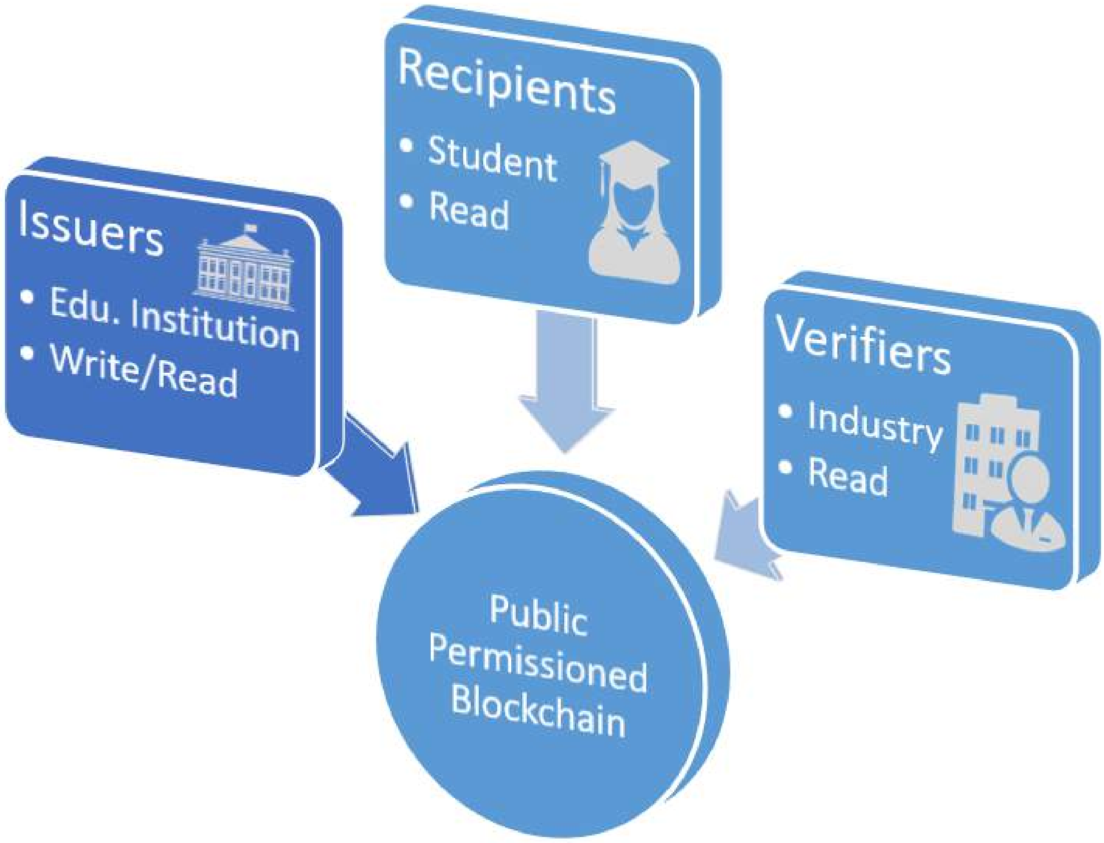
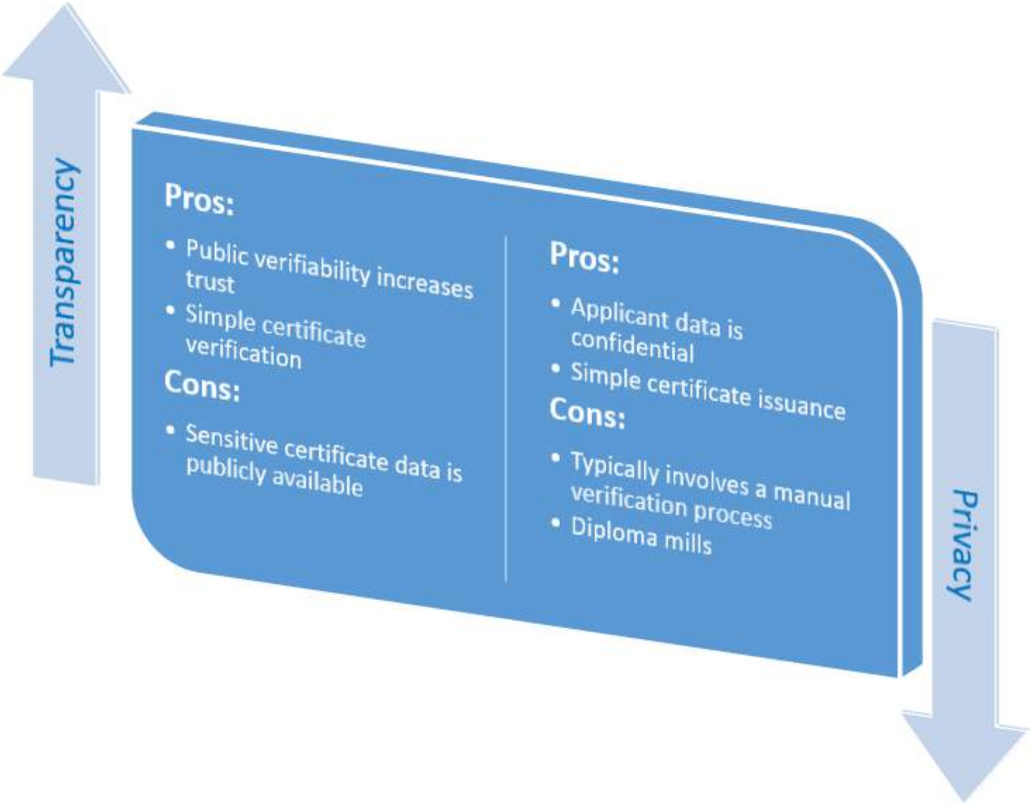


Figure 2 - Relation Between Stakeholders

While there is a need to rely on issuers' emitted certificates, there is no need to centralize consensus control at these nodes. Thus, all stakeholders in the network can contribute to the consensus process or have the option of also relying on these institutions to determine network consensus. A technical solution concentrating consensus on trusted institutions can lead to a partial network centralization, in which the inherent transparency and reliability benefits of a blockchain with decentralized consensus mechanisms can be sacrificed concerning performance and privacy. For example, there is no need to trust that an educational institution will issue in the blockchain certificates emitted by another educational institution. In addition to the non-inclusion (intentional or unintentional) can generate economic advantages for a given institution, which can further provide an information base enabling the mapping of the productive capacity of an institution.

Therefore, there are significant trade-offs that should be taken into consideration before choosing a technical option. For example, the trade-off between transparency and confidentiality is a relevant discussion to be considered, which also influences the blockchain type of deployment. While transparency is necessary to ensure that verifiers can rely on certificates issued, privacy is also essential to ensure that the data in the block cannot reveal information from recipients and institutions. For example, if certificates stored in a public permissioned blockchain are available for the general public, these could potentially be exploited as an information base for companies in the market-oriented field. For instance, it is possible to extract information such as name, age, gender, and profession and group this information into different categories that could be the target of an oriented-marketing. Therefore, caution must be taken concerning the access to certificate information, requiring a reading authorization of the principal interested in proving a certification – the job applicant (*cf*. Figure 3).



**Pros:**

- Public verifiability increases trust
- Simple certificate verification

**Cons:**

- Sensitive certificate data is publicly available

**Pros:**

- Applicant data is confidential
- Simple certificate issuance

**Cons:**

- Typically involves a manual verification process
- Diploma mills

Figure 3 - Trade-off Between Transparency and Confidentiality

On the one hand, if the transparency of certificates written by academic entities violates the privacy of applicants/students. The full confidentiality of a private permissioned database, on the other hand, creates data silos in which the use of a public ledger, such as blockchain, is not necessary. In this case, each academic institution has its own database in which it controls the certificates issued to its students, and access to this information is usually done through an institution-mediated request, which verifies that the student is the holder of the claimed degree. However, the need for trust in the academic institution issuing the certificates led to the *diploma mills* issue; thus, it is necessary not only the transparency concerning the issuance of certificates but also the accreditation of institutions accredited for writing in this public ledger.

A balance between total transparency and full confidentiality is necessary in order to be able to trust certificates issued in this global ledger and at the same time that the confidentiality of the applicants is preserved. Therefore, a possible way to preserve confidentiality while the verification/validation process is transparent to all stakeholders (*i.e.,* academy, industry, and applicant) involves storing identifiers of the respective certificates in the blockchain, and the certificate itself is either stored in a centralized database or directly given by the applicant to the industry employer. In this sense, in an approach based on a public permissioned blockchain, identifiers of the certificated can be generated using hash functions to create a digital representation of the certificate content. Hence, any attempt to include false information in the official document would produce a different hash than the original hash stored in the blockchain.

Since job applicants usually provide their CV to prospective employers (which contains information about their diplomas and certificates), it is also possible that the identifiers are included along with these certificates in the form of hashes or QR (Quick Response) codes. In this approach based on public and permissioned deployments, the certificate owner becomes responsible for revealing the confidentiality of its certificate while the original document, as issued by the academic institution, continues with its original and unaltered representation in the blockchain.

Another tradeoff to be considered is the relation between the reliability and performance aspects (*cf*. Figure 4), which is also the result of the discussion between centralization or decentralization. blockchain are naturally slower than any centralized database due to their complete replication of the data, and consensus mechanism. Not only there is a latency to synchronize the state in all node, but also the transaction performance is affected in temporal and spatial dimensions to keep a consensus in the network (*i.e.,* ensure that all nodes are in the same state). In this sense, the PoW algorithm has a fundamental importance to guarantee that the blockchain is completely distributed, that is, the nodes responsible for deciding which transactions should be in the next block are not predefined entities but chosen by a process that demands a computational effort of the elected node.

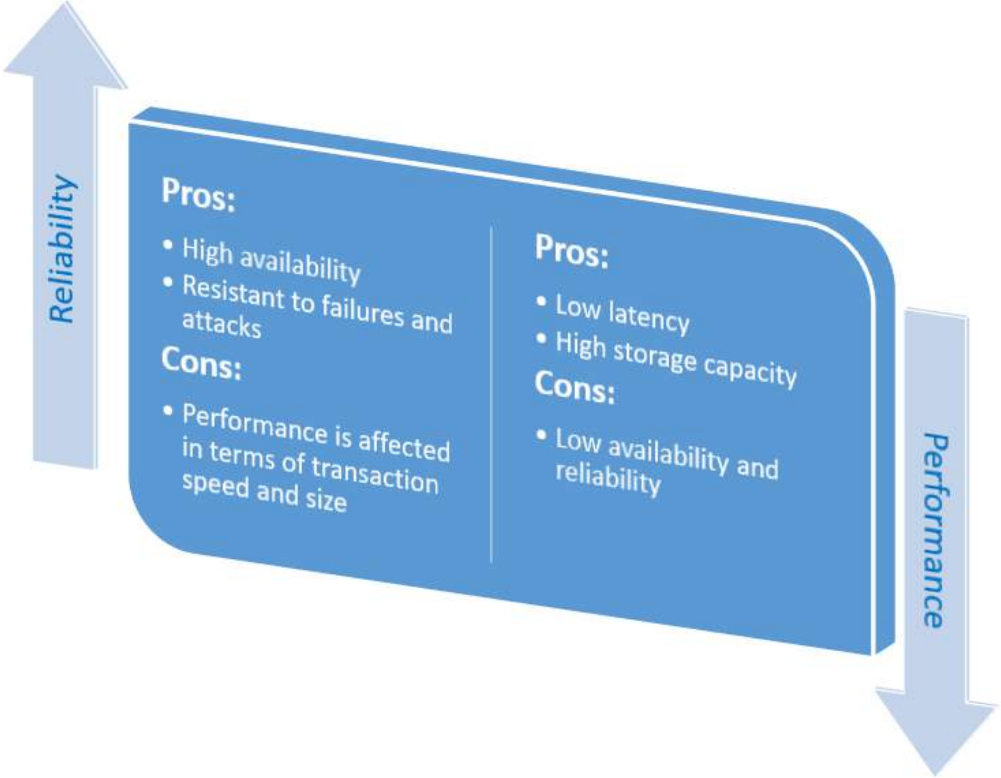

Reliability
Pros:
• High availability
• Resistant to failures and attacks
Cons:
• Performance is affected in terms of transaction speed and size
Pros:
• Low latency
• High storage capacity
Cons:
• Low availability and reliability
Performance

Figure 4 . Trade-off Between Reliability and Performance

Moreover, to issue and validate diplomas, the database reliability is a more relevant factor than the performance, because it is more important that the certificates are made available to employers at any desired time than ensuring that this access is made, for example, in the order of *ms* (Milliseconds) to *us* (Microseconds). This computational effort results in a loss of temporal performance not only in the computational dimension of a distributed system (there is a delay to compute a hash that satisfies the target hash) but also in the networking dimension with the need to transfer new blocks to all nodes in the network. Spatial performance (*i.e.,* storage space), however, depends on the size of the transactions (*e.g.,* identifiers of certificates, diplomas) to be included in a block as well as the maximum size defined for the block.

Based on an off-chain storage strategy, *i.e.,* storing diplomas and certificates in centralized databases and a checksum in the blockchain, it is possible to optimize spatial performance by including in a block a higher number of smaller transactions. A negative aspect of this approach is that the original content of the certificate or diploma will be stored in a centralized database (the educational institution), but the checksum proving its integrity will be available and unalterable for any verifier at the blockchain. Based on the practical aspect, job applicants (or diploma recipients) usually provide these diplomas to a possible employer, being possible for the verifier to calculate the diploma checksum and verify its integrity and authenticity.

Although naturally slower than centralized databases due to its the full replication of data, there are different consensus algorithms which offers a higher transaction throughput than PoW. Therefore, whenever it is possible to trust specific nodes in the network, it is also possible to replace the PoW algorithm by a consensus based on pre-selected entities. In case of blockchain tailored to handle academic certificates, in which write permissions are given to trusted educational entities (responsible for issuing diplomas), it could also be possible to rely on these entities to determine the network consensus based on a quicker algorithm than PoW. Thus, trusted nodes would replace the expensive election process of PoW and would be responsible for maintaining the network consensus.

However, the use of pre-selected entities to determine the network consensus results in a re-centralization of the network (Rodrigues et al. 2018; Karl and Gervais, 2017). In this sense, the use of Trusted Third Parties (TTP) makes the use of blockchain unnecessary and alternatives based on distributed databases may be a better option considering the tradeoff between reliability and performance. Although writing permissions are restricted to educational institutions, the process of verification and validation of transactions submitted by these entities can be based on PoW to guarantee the complete decentralization of the network. In this case, given that academic institutions do not generate certificates every second or minute it is not required to write academic certificates at every second or minute whereas academic certificates are generated on a larger temporal scale (*e.g.* days or weeks). Therefore, the prioritization of performance over reliability is not necessary for this application because it is necessary that written diplomas are available at any time a verification is necessary. A comparison concerning main operations and requirements is presented in Table 1:

**Table 1 - Comparison of Properties of Blockchain and Centralized Databases**

| **Properties** | **Public Blockchain** | **Centralized Databases** |
|---|---|---|
| **Operations** | Write (selected institutions), Read | Insert, Read, Update and Delete |
| **Replication** | Full replication | Master-slave |
| **Consensus** | Open to all nodes based on an election process | Pre-defined node(s) |
| **Requirements to Handle Academic Certificates** | | |
| **Participation** | Accredited institutions should be entitled to issue certificates | Any institution can issue certificates |
| **Integrity** | Emitted certificates are immutable | Certificates can be modified |
| **Privacy**<br>**Transparency** | Partially available with data stored off-chain storage and identifiers (checksum) stored on chain | Possible due to the private nature |
| **Performance**<br>**Reliability** | Highly available due to the blockchain full replication and slower in temporal and spatial dimensions | Partially available depending on the replication and faster in temporal and spatial dimensions |
| **Verification of Certificates** | Easy as certificate data is publicly available | Difficult as it is required permissions to check certificates integrity |

A blockchain is not ideal when there is a TTP or all involved parties are known and trust each other. For cases where exists a TTP or there is no need for disintermediation, a blockchain-based solution might become a problem for data confidentiality and performance of transactions. Thus, when parties are known and trusted, a traditional database with shared access is likely to be the most suitable option to address these issues. A public permissioned blockchain is necessary when public verifiability is required, but only some pre-defined parties can be trusted. For these cases, a central entity manages the membership of participants, being responsible for granting or denying permissions to a set of participants to read or write in the blockchain.

Moreover, existing approaches towards the handling of blockchain-based certificates can be classified in four different categories of solutions (Grech and Camilleri, 2017):

- **Proof of Existence**: the blockchain is used as a time-stamping solution to ensure that the certificate has not been modified since the first time the original document was stored. The proof of existence is based on hash of digital document and further interactions with the approach is not required after the document is stored in the blockchain.

- **Vendor as Notary**: these approaches also provide a proof of existence but processes of recording and verifying certificates on the blockchain are necessarily done via the proposed solution. Therefore, such solutions act as an intermediator between the academy, students and companies in a way that the access to the information is dependent of the solution.
- **Know Your Customer (KYC)**: provide a DApp (Decentralized Application - front-end or mobile app) that allow recipients to demonstrate the ownership of their certificates. While it facilitates access to stored data, solutions based on this approach usually require the data to be on their platform in a way that there is a reliance on the vendor to access information.
- **Digital Self-Sovereign**: similar to KYC in order to facilitate the verification of certificates, but certificates do not necessarily need to be of the same vendor. Therefore, there is no vendor-dependency in solutions based on this approach enabling individuals to share or verify these records. Nonetheless, records must be stored based on open standards and include the public key of recipients.

# 3 Landscape of Blockchain in Education

There are different proposals of the industry and academia for the use of blockchain in Education. This chapter aims to describe selected works, focused on educational certificates and diplomas, discussing how the technological choices can affect the tradeoffs presented in the previous chapter.

## 3.1 Blockcerts

Blockcerts is one of the first cases using blockchain to issue and verify diplomas (MIT Registrar, 2018). It is an MIT (Massachusetts Institute of Technology) initiative that proposes an open standard for issuing and verifying credentials on the Bitcoin or Ethereum blockchain. Then, stored diplomas that follows the Blockerts standard can be accessible via a mobile app named “Blockerts wallet”, which enable recipients (students) to get a tamper-proof version of their degree which can be shared with verifiers (e.g., employers, schools, family, and friends).

As blockchain is an enabler of transparency (and trust as a consequence) and solutions such as Bitcoin and Ethereum are becoming more popular, several related blockchain-based proposals are expected. Therefore, Blockcerts not only proposes an application to certify diplomas, but a standard on which additional proposals could be based. However, Blockcerts’ proposal rely on permissionless public blockchains (e.g., Ethereum and Bitcoin), implying that unrecognized institutions may become eligible to issue certificates, which may result in the issue of diploma mills.

Blockcerts deals with the tradeoff of privacy and transparency by registering a checksum of the original diploma on-chain and storing the content of the off-the-line diploma. Therefore, at the same time that it is possible to publicly verify a diploma, its data remain confidential.

## 3.2 Disciplina

With a similar goal to Blockcerts, Disciplina (Kuvshinov et al., 2018) aims to create a blockchain environment to register academic achievements where an employer would be able to search for potential candidates to a job in a “trusted” environment. Therefore, in addition to providing the certification platform, it focuses on creating a marketplace for Human Resources (HR) in which employers can, in theory, be assured that potential candidates have their skills certified.

Instead of basing its platform on existing blockchain projects, Discipline creates its blockchain in which the virtual environment running on the distributed nodes is simplified to support the application needs

(Kuvshinov et al., 2018). Therefore, the support for programmable/smart contracts such as in Ethereum is not possible and their structure is specifically tailored to support records of Universities, small education institutes, schools, and other educational platforms.

The authors justify the architectural choice of a mix between traditional DB and public permissionless blockchain by stating that a public permissionless blockchain is economically inviable. Every update on a student grade would have to be recorded on a blockchain, which would increase the amount paid in transaction fees. Therefore, as discussed in the previous Chapter, Disciplina uses an approach based on two layers: (a) a traditional private DB to maintain student data confidential and (b) a public blockchain to store necessary information to validate integrity and authenticity of private blocks.

The goal is that frequent updates (*e.g.*, grades or evaluations) on the student grades are performed on the private layer, and less frequent updates (*e.g.*, certificates) are registered in a public blockchain. Therefore, student and institution data are kept private, and only the diploma checksum is stored in the blockchain, which is a similar approach to Blockcerts (MIT Registrar, 2018). The differential is just the ecosystem that allows employers to search for verified candidates.

## 3.3 Sony Global Education

Sony, through its subsidiary Sony Global Education (SGE) (Sony Global Education, 2018), announced its participation toward digitization of the certification process in education. In partnership with IBM, SGE seeks to transform the certification process in Japan based on IBM's cloud-based blockchain (Haswell, 2018). The operation of the platform occurs similarly to (MIT Registrar, 2018; Kuyshinov et al. 2018), enabling institutions to record assessments of students and certificates and diplomas, and also companies looking to hire verified students, in a similar approach to Disciplina (Kuvshinov et al., 2018).

The IBM blockchain is based on the Hyperledger Fabric, a permissioned blockchain delivered via the cloud to SGE. However, if the blockchain runs through a cloud platform, then its necessity needs to be reconsidered. When trusting in a TTP (*i.e.,* the cloud platform), the use of a blockchain becomes unnecessary; thus, in this case, the employment of a traditional database becomes more efficient (Rodrigues et al. 2018). In addition to institution and student privacy considerations, the platform’s reliability becomes similar to a traditional distributed database - depending on the number of replicas available. However, with the employment of a traditional database, one gains the temporal and spatial performance, which allows the complete record of the academic history of students and institutions participating in the platform.

As with a different approach than the previous proposals, SGE offers the platform together with the government of Japan. Therefore, it is possible to ensure that only recognized and properly accredited institutions can write on the platform and thereby prevent unrecognized institutions from issuing diplomas.

## 3.4 UZHBC

The University of Zurich (UZH) began the process of digitizing their certificates with a feasibility study and a proposal based on a prototype (Gresch et al., 2018). This involved in a first step the analysis of the current UZH certification process, which included an investigation of requirements as well as interviews with stakeholders of each faculty. The analysis revealed that in addition to technical integration challenges, there are governance challenges that could impair the adoption process. For example, each UZH faculty is independent when it comes to the issuance of diplomas, and their respective dean's office is responsible for this task as an independent entity that has its conditions for graduation. However, the independence of faculties makes a decentralized blockchain-based system justifiable by ensuring that each UZH faculty can write their degrees independently of a central campus administration, and transparently to all faculties.

Then, it was performed a feasibility analysis to integrate the blockchain-based certification into the current system. After the approval of a certificate or diploma in each UZH faculty, a digital representation is generated in order to print the physical diploma in paper form. From this file of which the diploma in paper is printed, the UZHBC system calculates a hash which refers to this file in order to store in the blockchain. The hash function used in this approach is a SHA-3 with a length of 256 bits. SHA-3, unlike MD5, is considered collision resistant, which means that the chance that two different input values produce different output values is very high. Hashes can be used to prove the authenticity of software artifacts. In this case, one speaks of checksums. In this way, the student's privacy is guaranteed, as well as the storage in the blockchain is preserved.

## 3.5 BCDiploma

BCDiploma (BCDiploma, 2018) is a French initiative to certify diplomas that relies on the Ethereum (Wood, 2014) blockchain. The approach proposes to balance transparency and confidentiality in a similar manner to the ones seen in Disciplina, Blockcerts, and UZHBC. The blockchain is used in this context to store identifiers of the original documents, not revealing any data of the original documents. Thus, a hash/checksum of the original document is created in the implemented DApp and then stored in the Ethereum blockchain. Also, concerning the selection of accredited institutions, BCDiploma requires a third party so-called “Validator” that acts as an identity service to register accredited institutions as issuers in their framework.

The entire BCDiploma ecosystem consists of the DApp provided to accredited institutions, and a middleware layer called EvidenZ (Evidenz, 2018), which is responsible for encrypting diplomas and storing diploma hashes on the Ethereum blockchain. The EvidenZ operate in a similar way than Blockcerts, but it focuses on certifying data rather than focusing on the certification of diplomas. For this, the framework works as a Software-as-a-Service (SaaS) acting as a request-management middleware between the DApp and the blockchain. However, by relying on middleware acting as a TTP, the use of blockchain as a backend for storing records may become unnecessary. For example, if there is a relationship of trust between the educational institutions and BCDiploma, there is also the possibility of eliminating the use of blockchain, making the access to the identifiers of the diplomas direct to the EvidenZ framework.

## 3.6 Education Network of Greece (GRNET)

As with a similar approach than Blockcerts, the National Research and Education Network of Greece (GRNET) launched in 2017 a pilot project to verify student diplomas based on the Cardano blockchain (Amy Castor, 2018; Cardano 2018). The GRNET DApp will be built on a private or permissioned ledger version of Cardano, which differs from a public blockchain where anyone can join in and participate. With this, it is expected that only authorized educators can participate in this blockchain.

The goal is to create a system that can verify student diplomas on Cardano aiming to reduce the manual verification process and cases of fake degrees. Also, the GRNET project differs from Blockcerts in the sense that it can store not only hashes of diplomas, but also the entire verification process. Therefore, each step in the verification process will be stored in the blockchain to have the traceability of the requests and answers of verification of diplomas. Although there is no definition as to the blockchain model to be deployed (private or permissioned), the GRNET will operate similarly to other projects by storing a checksum of diplomas to preserve confidential recipient (students) data.

Concerning the trade-off between reliability and performance, GRNET is able to be more performant than others Proof-of-Work (PoW) based blockchains. Cardano (Cardano, 2018) uses a Proof-of-Stake (PoS) consensus algorithm in its current version (Ourobouros) that is able to achieve a higher transaction throughput than PoW blockchains by relaying on the entities with more stake at the network to issue new blocks. Therefore, instead of using the power of computing hashes as a way to elect a leader as seen in PoW, the creator of the next block is chosen via its resources at stake in the network.

## 3.7 Edgecoin

Edgecoin (Djafari and Gerdon, 2018) aims to differ from other blockchain education projects by targeting in a Business-To-Business (B2B) model instead of building a content-centric blockchain. The targeted B2B stakeholders are academic institutions, e-learning platform, independent education advisors, and corporate learning and talent management platforms. However, Edgecoin uses a technical approach that is similar to the others (*e.g.*, Blockcerts, Disciplina, BCDiploma) by storing a hash of the diploma in the blockchain. Specifically, Edgecoin uses the Ethereum network as backend to store diploma hashes and IPFS (Benet, 2018) (InterPlanetary File System) to store original diplomas in digital manner.

IPFS is a platform that enables the decentralized storage of files across the Internet. Edgecoin uses IPFS to store metadata such as long descriptions, images, scancopies linked to the certificate which are then linked to the Ethereum smart contract using a generated IPFS hash. Based on IPFS, Edgecoin provide a completely decentralized solution that, in terms of the trade-off between transparency and confidentiality, may introduce risks of data leaks by storing confidential (even encrypted) diploma data in a decentralized fashion.

## 3.8 Open Source University

The Open Source University (OS University) tries to bridge the gap between academia, industry, and students by using a blockchain-based solution (Open Source University, 2018) similar to Edgecoin. OS University provides a decentralized solution based on the combination of IPFS and blockchain, accessible via a DApp called OSU, that provides an interface to the Ethereum network. By using IPFS, users of the OSU DApp will have their personal information stored in a decentralized manner, but the information will be encrypted. The access to the information will be granted only by the owner of the information to a specific requester.

OS University, however, does not innovate the process that can influence trade-offs between transparency and privacy, and reliability and performance. In this sense, the solution presents a very similar approach to that used in Edgecoin, with the complete decentralization of the information stored by the solution. It should be noted that the information stored in IPFS, even though encrypted, is not under the domain of the academy or the student.

## 3.9 Gräter *et al.*

The FIT (Fraunhofer Institute for Applied Information Technology) (Gräter et al., 2018) proposed an open platform for securely issuing, verifying, and sharing academic credentials based on the blockchain. The system presents a similar design to OS University (Open Source University, 2018) and Edgecoin (Djafari and Gerdon, 2018) combining a front-end DApp where certifiers, learners and employers can interact with Ethereum blockchain and IPFS. While Ethereum holds the identification of certification authorities and certifiers (educational institutions), IPFS is used as an extended storage linked to the Ethereum identification to store the full profile of these entities.

Differently from OS University and Edgecoin, the FIT's system comprehends in the design functions of accreditation authorities, whose function is to validate which academic institutions are eligible to issue certificates in the platform. However, in terms of transparency and confidentiality trade-off the platform maintains the privacy of learners by using the same approach than (Djafari and Gerdon, 2018; Gräter et al. 2018) by storing checksums in blockchain while confidential data is kept off-chain.

## 3.10 CredenceLedger

CredenceLedger (Arenas and Fernandez, 2018) offers a mobile application to verify diplomas based on MultiChain (MultiChain, 2018), an open platform to build permissioned blockchains. The authors justify the choice for a permissioned blockchain to avoid the expensive mining process required by public permissionless blockchains (*e.g.,* Bitcoin and Ethereum), transaction fees, and the limited storage capacity. Therefore, MultiChain enables a faster transaction throughput as well as an increased storage capacity, which is used by CredenceLedger to store diplomas as streams of key-value pairs. Keys are identifiers in the MultiChain ledger and values are checksums of original diplomas.

Although the use of permissioned blockchains favors performance and confidentiality aspects, it imposes restrictions on reliability and transparency characteristics which are critical toward the establishment of trust among the stakeholders (*i.e.,* education institutions, companies and students). Transparency is the most important factor in the digital certification ecosystem since companies desiring to hire applicants need to clearly verify the origin and authenticity of the diplomas issued on this platform. In this sense, the use of a distributed database developed precisely for this purpose (*e.g.,* Redis) could provide an alternative with higher performance than MultiChain.

## 3.11 Discussion

A comparison of the different approaches used toward a solution for the management of blockchain-based certificates is presented in Table 2. The privacy of the student data in the certificate/diploma is the most essential requirement that drives technical decisions concerning the blockchain type (permissioned or permissionless) and how the actual diploma is stored off-chain. In this regard, all works have this concern reflected in its design so that the data exposed for public verification (*i.e.,* on-chain) do not disclose sensitive student information.

A common alternative is to make use of public permissionless blockchains to store only an identifier or checksum of the original diploma (which allows companies to verify the authenticity of the diploma using a DApp - front-end or mobile application), while the original diploma is stored either in a traditional database or in a decentralized file storage (*e.g.,* IFPS). Next, upon receiving a copy of the digital diploma, a company wishing to verify the authenticity of the document can check whether the checksum is the same of the one publicly available on the blockchain.

Moreover, approaches based on public and permissionless blockchains need to control which educational institutions that can issue valid certificates. This is presented in Table 2 in the permissions to issue certificates column, which can be realized using (1) smart contracts to declare which accounts are able interact with write permissions or (2) off-chain via an overlay network. Although everyone can interact with the blockchain in (1), only authorized accounts can interact with a smart contract to create or revoke emitted certificates. In (2), the same approach is used, but the access control of which accounts can issue valid certificates is done off-chain in a network over the blockchain.

As with a different alternative to increase the level of privacy, there are approaches such as Sony Global Education (Sony Global Education, 2018), GRNET (Amy Castor, 2018) and CredenceLedger (Arenas and Fernandez, 2018), that aim to offer more centralized blockchain solutions at different levels. Although offering a better balance between performance and confidentiality, the use of blockchain in some cases may become questionable as there is also the possibility of using a traditional distributed database whose read rights are publicly available. Data immutability is a point that could differ private blockchains from traditional distributed databases, but, in practice, a private blockchain can be changed as long as the participants of the network agrees.

Table 2 – Blockchain Type and Off-chain Storage

| **Work** | **Blockchain Type** | **Blockchain** | **Certificate Storage** | **Permissions to Issue Certificates** |
|---|---|---|---|---|
| **Blockcerts** | Permissionless | Bitcoin, Ethereum | Traditional DB | Off-chain overlay |
| **Disciplina** | Permissionless | Own Blockchain | Own Blockchain | Smart Contract |
| **UZHBC** | Permissionless | Ethereum | Traditional DB | Smart Contract |
| **BCDiploma** | Permissionless | Ethereum | Traditional DB | Smart Contract |
| **Edgecoin** | Permissionless | Ethereum | IPFS | Smart Contract |
| **OS University** | Permissionless | Ethereum | IPFS | Smart Contract |
| **Gräter *et al.*** | Permissionless | Ethereum | IPFS | Smart Contract |
| **Sony Global Education** | Permissioned | IBM Hyperledger | Traditional DB | Selected institutions |
| **GRNET** | Permissioned | Cardano | Traditional DB | Selected institutions |
| **CredenceLedger** | Permissioned | MultiChain | Traditional DB | Selected institutions |

Approaches involving public permissionless blockchains (*e.g.,* Ethereum (Wood, 2014) and Bitcoin (Nakamoto, 2008)) make use of on-chain identifiers of diplomas that are stored off-chain (*e.g.,* in traditional databases). Also, the choice for off-chain storage approaches is seen with smaller variants in Blockcerts (MIT Registrar, 2018), Disciplina (Kuvshinov et al., 2018), UZHBC (Gresch et al., 2018), BCDiploma (BCDiploma, 2018), EdgeCoin (Djafari and Gerdon, 2018), OS University (Open Source University, 2018) and Gräter et al., 2018, which can allow a higher or lower level of decentralization. While fully decentralized solutions are mostly based on IPFS making off-chain stored diplomas to be outside the issuer's domain, centralized solutions make use of traditional databases for the storage of digitized diplomas and only the on-record registration of the original files.

In this scenario, a discussion about the need for a fully decentralized solution is necessary since original diplomas are stored outside the domain of the issuer. In solutions like EdgeCoin (Djafari and Gerdon, 2018) and OS University (Open Source University, 2018), for example, original diplomas are encrypted with the recipient's (students) public key before being stored in IPFS. On the one hand, this enable the student to control which verifiers can access the data of the original diploma, whose authenticity can be verified by IPFS-hash stored in the blockchain. On the other hand, even if diplomas are stored in an encrypted manner they will be outside of the issuer's domain, which can imply in privacy concerns. However, such verification can be performed in two different ways that preserve the privacy of the data contained in the certificate. In the first, the applicant can provide the certificates to employees, who can verify through the DApp the authenticity of the document. In the second, the employer in possession of the curriculum provided by the applicant, can request the institution of education to verify the certificate.

The choice for a permissioned blockchain means that only authorized institution has permissions to create blocks of information. On the one hand this option removes constraints regarding the performance and confidentiality imposed by the use of public blockchains, but on the other hand it also takes away its benefits concerning immutability and reliability. Permissioned blockchains do not necessarily mean that selected academic institutions should manage the nodes responsible for the creation of blocks, which can be managed by specialized companies such as the IBM HyperLedger used by Sony Global Education (Sony Global Education, 2018). However, the use of blockchain in this specific case becomes questionable because there is a relationship of confidence in the entity managing the writing of transactions, implying that a distributed database could be a more viable alternative. However, the fact that the blockchain is permissioned not only in the sense of limiting those who can issue blocks, but also concerning educational institutions that can issue diplomas in this permissioned chain, does not mean that this blockchain should be deprived in the sense of limiting the reading rights. Reading permissions must ideally be open to the general public so that companies wishing to verify the authenticity of diplomas can perform such task in a free manner, without requesting reading permissions.

Based on the application requirements *i.e.,* the handling of academic certificates on the blockchain, it is straightforward that among the requirements performance is not more relevant than privacy. For example, having a diploma written in blockchain with the best possible temporal performance is not more important than this diploma does not relieve private information of the students. Furthermore, since both approaches (permissioned and permissionless) should ideally grant public reading permissions, it becomes necessary to use the same on-chain storage strategy in both approaches to hide confidential information. In this regard, the trade-off between reliability and performance can have a greater tendency for reliability in the sense that issued diplomas need to be ideally immutable and always available whenever a verification is necessary. The major challenge lies in the trade-off between transparency and confidentiality since the public visibility imposes a greater tendency to prioritize confidentiality. Thus, the approach based on the use of hashes identifying an original document stored off-chain is paramount to make an efficient use of on-chain storage and to guarantee the integrity of the document without revealing confidential information.

In addition, it is possible to categorize the approaches according to the categories proposed in (Grech and Camilleri, 2017). Although the discussed approaches have the same goal, different approaches providing different alternatives are given to the stakeholders involved in the processes of storage, verification and (if necessary) revocation of certificates. Figure 5 presents a classification based on the description of its characteristics and the similarity with the categories discussed in (Grech and Camilleri, 2017). In addition, the figure differentiates these categories into two dimensions in terms of vendor independence and ownership of recipient certificates. While the vendor independence relates to the access, display, and verification based on open-source standards, the recipient ownership means that individuals control the private keys that allow them to demonstrate ownership of money or their digital records. A third dimension shows that the approaches in the upper quadrants, proposed by the academy, favors vendor independence while the lower quadrants favor creates a vendor's lock-in.

Also, it is observed that some solutions can fit into more than one category. For example, OS University (Open Source University, 2018) can be classified as KYC as it provides a solution in which recipients are able demonstrate the ownership of their certificates, as well as a Vendor as Notary solution since the processes of issuing and verifying diplomas must rely on the OS University platform. In the case of Blockcerts (MIT Registrar, 2018), classified as a self-sovereign solution, the approach provides not only an open ecosystem, but also standards in which these certificates can be recognized by different platforms that implement this standard. This approach favors the recipient who can prove without intermediaries the authenticity of their certificates.

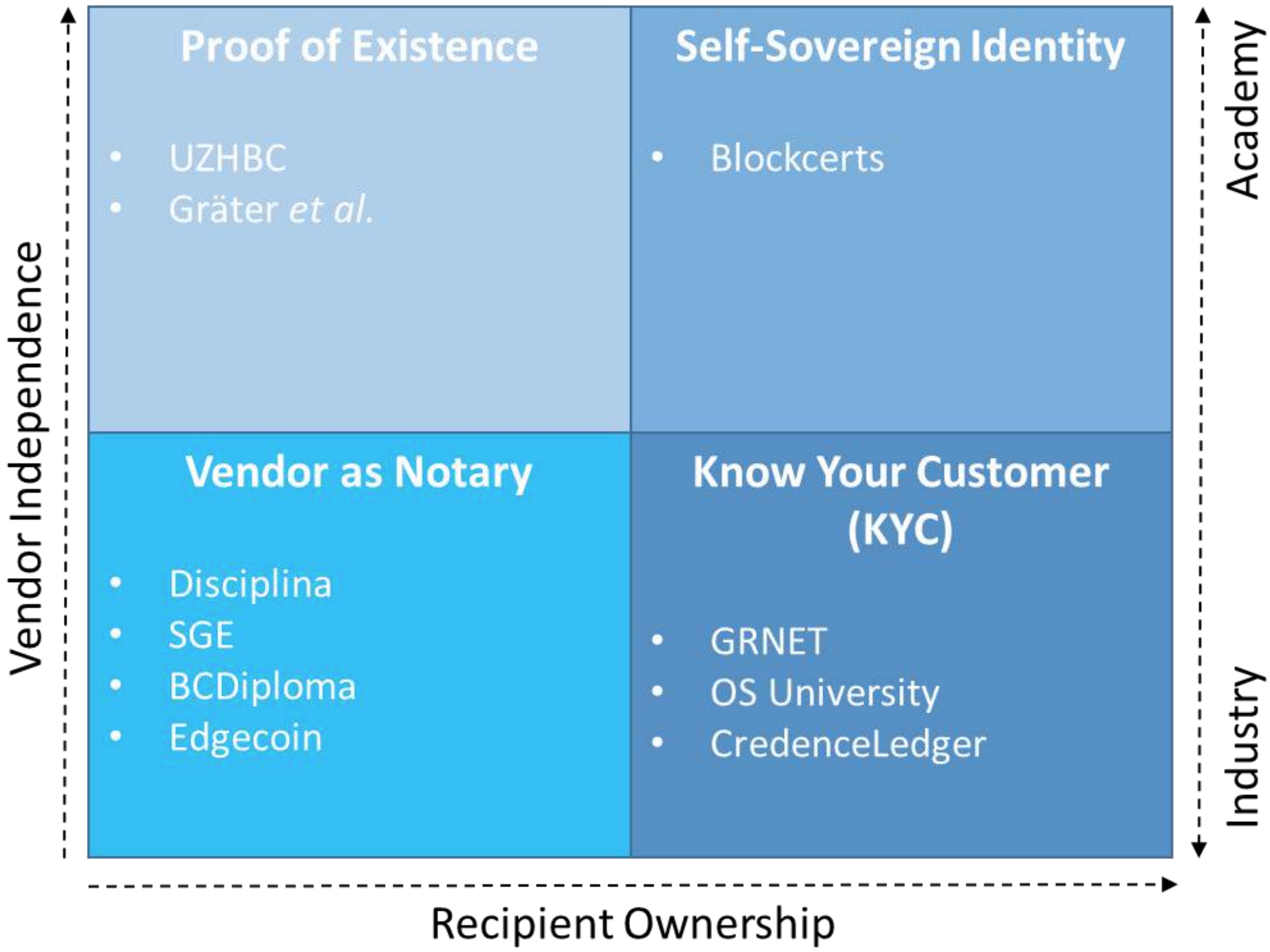


Figure 5 - Classification of Approaches (adapted from Grech and Camilleri, 2017).

With the aim of making the diploma verification process more dynamic, UZHBC (Gresch et al., 2018) and Gräter et al., 2018 propose solutions using blockchain integrated into their university system to facilitate the issuance and verification of their certificates. The UZHBC proposal, for example, is an initial work toward the automation of the processes of verifying certifications, currently manual and time-wise costly, replacing by a process based on blockchain in which the companies themselves can easily verify the integrity of certificates issued by the university without the need of permissions. In this case, the purpose is solely to use blockchain as a public and global proof of existence storing a hash that can be used to proof the integrity of the original document.

In the lower quarters are the industry solutions categorized as Vendor as Notary and KYC. While the former categorizes approaches that provide proof-of-existence imposing a vendor lock-in on the stakeholder's interaction with the stored certificates, the latter also performs the lock-in but provides in addition a greater freedom for the recipient to prove the authenticity of diplomas. Causes for vendor lock-in could be understood as an attempt by industry companies to dominate the certificate verification market which was recently revolutionized by blockchain. Thus, it is natural that companies propose their own ecosystems involving solutions for on-chain and off-chain storage as well as exclusive front-end or mobile application access for validation.

## 4 Challenges and Opportunities

The major problem that motivates the existence of numerous blockchain-based approaches to provide more transparency and integrity of educational certificates is related to the increasing number of fraudsters and fraudulent institutions and the increasing number of non-accredited educational institutions seeking to meet the demand for higher degree diplomas. Therefore, the *diploma mills*, as previously defined, are these fraudulent institutions that provide counterfeit certificates often acting in a similar way than a recognized and accredited institution. Therefore, it is possible to classify the major problems in two categories:

1) Prevent certificates issued by recognized and accredited institutions from being modified.
2) Prevent unrecognized and accredited institutions from issuing certificates.

While existing proposals are mostly focused on providing technical solutions toward the optimization of spatial and temporal performance, (1) as well as to prevent that information contained in certificates are modified, (2) it is necessary that these same approaches seek solutions to validate which institutions are recognized and accredited. Since diploma mills may act similarly, issuing and recognizing fake certificates, it is necessary that solutions act with government agencies responsible for the regulation of these educational institutions.

A third problem is related to the standardization of certificates issued in the blockchain. This problem is the main focus of Blockcerts (MIT Registrar, 2018), which proposes not only the platform in which the recipient can hold its certificates, but a universal standard where educational institutions can implement to issue blockcerts-compliant certificates. With the emergence of many diverse proposals and ecosystems operating in an isolated way, the challenge becomes the interconnection of isolated diplomas in different blockchains. However, this is not an exclusive problem of the blockchain-based certification, but a general problem of the so-called “Blockchain 4.0” that addresses the integration of blockchain solutions with industrial applications (*e.g.,* supply chain, healthcare). Therefore, the major opportunities in the field of managing blockchain-based certificates can be defined by the following aspects:

1) The definition of standards to issue certificates in different blockchain solutions.
2) Development of solutions that can interconnect different blockchains based on standards.

Blockchain which was initially conceived to promote disintermediation and a greater interaction between different stakeholders operating in isolation. However, it is becoming a scenario where different stakeholders operate in different blockchain networks that are closed in their own ecosystem. Thus, the definition of standards becomes at a first sight a fundamental aspect to make these different isolated networks to communicate once again promoting the desired transparency and integration. Then, the development of new solutions as well as the adaptation of existing solutions to operate based on standards become necessary.

Another challenge is related to the self-sovereign identities, which deals with the decentralization of recipient identities and credentials, so that they can also own their certificates issued in the blockchain. Thus, it would be possible to provide a complete freedom so that the recipients of the diploma can make verifiable claims in their curriculum vitae independently of a vendor or educational institution. However, the realization of self-sovereign certificates requires the existence of a standardization, which may describe, for example, how an object should encapsulate identity related data and also the functions which can be performed on the object to grant verifiability permissions on certificates.

# 5 Final Considerations

This chapter presented an overview of works oriented to the handling of certificates based on blockchain, presenting and discussing their characteristics from a technological point of view. Based on the different blockchain types and the different characteristics they can provide; it was discussed how the main approaches addressed trade-offs between the requirements to handle certificates in a publicly available database.

In conclusion, among the discussed requirements there is in common concern with data confidentiality in relation to the transparency that blockchain naturally offers. This concern is reflected in the technical choices of all approaches, resulting in a common goal that only certificate identifiers are publicly exposed; and the difference lies in how these certificates are stored off-chain. Blockchain-based solutions are an evolution in the handling of certificates presenting technologically viable solutions against certificate forgery. However, there are still efforts to be done both from a technological point of view (*e.g.,* standardization and interoperability) and organizational (*e.g.,* accreditation and recognition of educational institutions).

## 6 References

Hanna Park. “*Diploma Mills: Accreditation and Quality Assurance*.” World Education Services (WES). URL: https://wenr.wes.org/2017/12/diploma-mills-9-strategies-for-tackling-one-of-higher-educations-most-wicked-problems Accessed: 22/10/2018

Musee, Nicholas Mwaniki. "*An Academic Certification Verification System based on Cloud Computing Environment.*" PhD dissertation, University of Nairobi (2015).

Jeremy S. Alder. “*Diploma Mills; How to Recognize, Avoid Them.”* URL: https://www.collegechoice.net/diploma-mills/ Accessed: 22/10/2018.

Grech, Alexander, and Anthony F. Camilleri. “*Blockchain in education*.” JRC Science for Policy Report. European Comission. (2017).

Jirgensons, Merija, and Jānis Kapenieks. "*Blockchain and the Future of Digital Learning Credential Assessment and Management*." Journal of Teacher Education for Sustainability 20.1 (2018): 145-156.

Nele Breuls, Cedric Van Daele, Kim Vanelderen, Dorthe Pedersen, Gunnar Vaht, Marina Klementjeva, Luca Lantero, Chiara Finocchietti, Vera Lucke, Ana Mateus, Vasco Rodrigues, Erik Johansson, Samir Gabro. (2018). “*Guidelines on Diploma Mills and Document Fraud for Credential Evaluators.”* FRAUDOC Project. European Comission.

Jerinas Gresch, Bruno Rodrigues, Eder Scheid, Salil S. Kenhere, Burkhard Stiller. “*The Proposal of a Blockchain-based Architecture for Transparent Certificate Handling”.* BSCT 2018: 1st Workshop on Blockchain and Smart Contract Technologies. Berlin, Germany, July 18, 2018.

Angrave, D., Charlwood, A., Kirkpatrick, I., Lawrence, M., & Stuart, M. (2016). “*HR and Analytics: Why HR is Set to Fail the Big Data Challenge*”. Human Resource Management Journal, *26*(1), 1-11.

Scholz, T. M. (2017). “*Big Data in Organizations and the Role of Human Resource Management”* (pp. XVII-pp). PETER LANG LTD International Academic Publishers.

Warasart, Maykin, and Pramote Kuacharoen. "*Based Document Authentication Using Digital Signature and QR code.*" In 4th International Conference on Computer Engineering and Technology. International Proceedings of Computer Scienceand Information Technology, pp. 94-98. 2012.

Nakamoto, S. (2008). “*Bitcoin: A Peer-to-Peer Electronic Cash System.* “ URL: https://bitcoin.org/bitcoin.pdf

Rodrigues, B., Bocek, T., & Stiller, B. (2018). "*The Use of Blockchains: Application-Driven Analysis of Applicability*”; in: Pethuru Raj, Ganesh Deka (Edt.), Blockchain Technology: Platforms, Tools and Use

Cases, Volume 111 (Advances in Computers). Springer, Waltham, MA, U.S.A, No. 111, September 2018, ISBN 978-0-128-13852-6, pp 1–22.

W. Karl, A. Gervais. (2017). "*Do you need a Blockchain*?" IACR Cryptology ePrint Archive: 375.

MIT Registrar's Oce: *"Digital Diploma Pilot Program FAQs".* URL: https://bit.ly/2JYw4zT Online. Accessed: 2018-11-22.

K. Kuvshinov, I. Nikiforov, J. Mostoyvoy, D. Mukhutdinov, K. Andreev, V. Podtelkin. *Disciplina: Blockchain for Education*. Yellow Paper. URL: https://disciplina.io/yellowpaper.pdf

Sony Global Education. URL: https://www.sonyged.com Online. Accessed: 2018-11-22.

Holli Haswell. "*Sony and Sony Global Education Develop a New System to Manage Student's Learning Data, Built on IBM Blockchain*". URL: https://www-03.ibm.com/press/us/en/pressrelease/52970.wss Online. Accessed: 2018-11-22.

BCDiploma. "*Diplomas Certified on the Blockchain."* URL: https://www.bcdiploma.com/ico/img/BCD-WhitePaper_last.pdf Online. White Paper. Accessed: 29.11.2018

Wood, G. (2014). "*Ethereum: A Secure Decentralised Generalised Transaction Ledger*". Ethereum project yellow paper, *151*, 1-32.

Evidenz. "*Certified, Encrypted Data Available On-Demand*". URL: https://www.evidenz.io/ Online.

Amy Castor. "*Cardano Blockchain's First Use Case: Proof of University Diplomas in Greece*". January, 2018. URL: https://bit.ly/2DVsrYt Online.

Cardano. "*Cardano Blockchain*". URL : https://www.cardano.org Online.

Kambiz Djafari, Max Gerdon. *"Edgecoin Blockchain as a Service in Education".* URL: https://drive.google.com/file/d/1C6Se1_IO_1-RCp_4jOohRyZXMBBJlqJu/view Online.

Benet, J. (2014). IPFS-content addressed, versioned, P2P file system. *arXiv preprint arXiv:1407.3561*.

Open Source University. *"The World's Academic & Career Development Ledger".* URL: https://os.university/static/open-source-university-edu-whitepaper.pdf Online.

Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C., & Wendland, F. (2018). Blockchain for Education: Lifelong Learning Passport. In Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET).

R. Arenas and P. Fernandez, "CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials," 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Stuttgart, 2018, pp. 1-6.

MultiChain. *"Open Platform for Building Blockchains"*. URL: https://www.multichain.com/

Online.