Research in Globalization 3 (2021) 100034

Contents lists available at ScienceDirect

Research in Globalization

journal homepage: www.elsevier.com/locate/resglo

Blockchain in international e-government processes: Opportunities for recognition of foreign qualifications ☆,☆☆

Christian Pauletto *

International University in Geneva (IUG), Switzerland

ARTICLE INFO

ABSTRACT

Purpose: Recognition of foreign qualification for authorising the exercise of a regulated professions gains importance in globalised economies and in international organisations such as the UNESCO. However, national procedures for such recognition have not yet experienced the transformative changes that occurred in other sectors of public administration. The study of "transborder digitisation" is still in its infancy. While governments consider the adoption of blockchain applications for the e-administration of trade-related procedures, for example customs procedures, it is timely to give some thoughts to recognition as well.

Aims: After explaining the role of recognition in international relations this article explores the features of recognition procedures that are relevant for the choice of a technology. It then aims to identify recognition authorities' needs in terms of administrative tools and to find out the options and potential benefits of blockchain technology in view of those needs. It aims to find whether there are reasons to select that particular technology rather than conventional methods. This is highlighted in a concrete description of what could be a possible configuration of a blockchain solution for recognition procedures. Since opportunities are always balanced by limitations, the article also inquires into ithe expected challenges in adopting a blockchain system between different countries' recognition authorities. The article's overall aim is to offer an assessment of blockchain technologies' potential in that field and to highlight developments in technology that could ease their adoption.

Findings: The article finds that the advantages brought by DLT technologies and the needed features of recognition processes coincide in several respects. However, some critical challenges and limitations for the application of blockchain in this field also exist. An adoption of that technology for that particular branch of public administration could occur provided that the technology continues to improve. Such improvements include interoperability, interface with other protocols and legacy databases, portability, and a higher degree of safety regarding privacy.

1. Introduction

> "the main discussions surrounding blockchain nowadays focus on the question of how to utilize this technology in other potential areas of use (i.e. beyond digital currencies) from a commercial and technological perspective."[1]

Distributed ledger technologies (DLT) are being implemented mainly in the financial sector (cryptoassets, online payments, money transfers, etc.). However, with time, technological developments and standardisation the potential for implementation of DLT could expand to almost any sectors. Compared to finance, and more recently logistics-related applications and electronic commerce, the research made on possible blockchain applications in the realm of intergovernmental cooperation, which could be coined "transborder digitisation" or "cross-border digitisation", is in its infancy. This article aims to stimulate the interest in the applications of blockchain in transborder administrative procedures by showing a concrete case, the official recognition of foreign qualifications by states for the purpose of the

☆ This paper was presented at the Research Workshop on Blockchain "Global Trade and Blockchain Forum" held by the World Trade Organization (WTO) in Geneva on 2–3 December 2019. Forum programme: <https://www.wto.org/english/res_e/reser_e/workshop_blockchain_21219_e.htm>. Presentation: <https://www.wto.org/english/res_e/reser_e/07_a_christian_pauletto_blockchain_and_global_trade.pdf>.

☆☆ Prof. Christian Pauletto is Associate Professor at the International University in Geneva.

* Address: International University in Geneva (IUG), International Center, 20 Route de Pré-Bois, 1215 Geneva 15, Switzerland
E-mail address: cpauletto@iun.ch

[1] Gürkaynak, Yılmaz, Yeşilaltay, and Bengi (2018).

https://doi.org/10.1016/j.resglo.2020.100034
Received 29 January 2020; Revised 13 December 2020; Accepted 13 December 2020
Available online 16 December 2020
2590-051X/

exercise of a regulated profession. The only digital applications that have been adopted in the context of recognition fall short of that. For example, the most mature and accomplished (in the opinion of the author) such application is the Recognition Finder application of the German recognition authority.[2] But though this website is most helpful to assist the holder of foreign credentials to understand the application process, to know which documents need to be filed and in what form, and to identify the competent authority and its contact details (including website and geolocalisation), it stops at the point of actually submitting the application.

To date no study or use case analysis has been published on the contribution of blockchain technologies for such recognition procedures. This piece intends to address this research gap.

1.1. Scope of the article

It may help to clarify at the outset what this piece is not about. This article doesn't comment on policy choices and directions in terms of official recognition, e.g. questions as to whether, how and to what extent recognition should be pursued. Nor does it focus on academic recognition, (e.g. between universities or academic programmes) or on computerised systems for issuing and checking university degrees, though those two aspects are part of the context of this article.

The focus of this research is on the adoption of a particular tool by a public administration within an established national policy and practice of recognition. Administration of recognition processes involves a degree of cooperation with authorities abroad. Given that the term "recognition" is used in several areas of international relations it is helpful to propose a definition of its meaning in the context of this article. To best seize the meaning of recognition in that context we propose the following definition:

Recognition of qualifications is a procedure within a State's legal framework and administered by a government authority or a delegated body for the purpose of verifying qualifications of holders of professional credentials earned abroad, such as academic degrees, training or experience, and leading to a decision authorising (or not) the applicant to practice under its jurisdiction in a regulated professions.

The above proposed definition considers the broader process leading to recognition, rather than focussing on the formal administrative act materialised in the acceptance of an application as the UNESCO does.[3] Because of this focus on the process rather than on one of its possible outcomes this definition also encompasses the denial of a recognition. Arguably, recognition could also extend to the withdrawal of a prior recognition decision. The distinction between defining something with respect to its outcome vs. the process leading to it is not unique to recognition.

1.2. Context and purpose of official recognition of professional qualifications

With globalisation, the shortening of distances, mobility of skills and international division of labour, the demand for official recognition of foreign qualifications is on the rise worldwide. At the same time, education itself is increasingly internationalised, as evidenced in several chapters of Maringe and Foskett (2013), which means that an increasing number of students will later return to their home country with a foreign certificate.

Another phenomenon is that whilst recognition practices and policies differed widely across national recognition authorities a few decades ago, over time a sort of convergence, or the emergence of sets of "good practices", in official recognition procedures seems to take place, at least at regional levels.

In a world that becomes both more competitive and technology-driven, individuals are increasingly aware of the importance of acquiring and offering personal competences. Hence the number and diversity of degrees, certificates and licenses on the market is growing.

These trends translate in an active interest for recognition issues by international bodies such as the UNESCO (see Section 3.4), which has just opened for signature its Global Convention on the Recognition of Higher Education Qualifications in September 2019 (hereinafter, the "Global Convention").[4]

Proofs of concepts or actual applications have been developed for a number of procedures that share analogies with recognition of professional qualifications in that:

- they involve a mix of governmental authorities and private actors,
- they aim a fulfilling an official administrative procedure,
- they apply (at least in part) at transborder level,
- their rationale is to facilitate trade.

Among those "transborder digitisation" projects the customs sector takes the lion share, including one particular aspect that is very similar to the topic of this article, namely the transborder recognition by an authority of a so-called "authorised economic operator" (AEO) from another jurisdiction. The major pilot on mutual recognition of AEOs, called CADENA, was launched by the Inter-American Development Bank (IDB) with the support of the World Customs Organization (WCO) and covers a number of Latin American countries.[5] Another pilot called *bCONNECT* was launched by Brazil,[6] and was recently extended to other MERCOSUR countries.[7] Similar schemes exist for the acceptance, respectively the mutual recognition, of controls on goods performed by foreign authorities. But rather than being implemented in stand-alone they are mere parts of broader blockchain-based supply management systems (B2B and G2G). A prominent example is *TradeLens*, launched by private companies with the initial participation of customs authorities in the Netherlands, Saudi Arabia, Singapore, Australia and Peru.[8,9]Other applications exist in the field of

[2] See Anerkennung in Deutschland, <https://www.anerkennung-in-deutschland.de/de/interest/finder/profession>.

[3] See definition 1(h) of the UNESCO Recommendation on the Recognition of Studies and Qualifications in Higher Education of 13 November 1993: "'recognition' of a foreign qualification in higher education with a view to the practice of a profession means acceptance by the competent authorities of the professional preparation of the holder for the practice of the profession concerned, without prejudice, however, to the legal and professional rules or procedures in force in the States concerned and provided the holder would be entitled to practice the same profession in the State in which the professional preparation and qualification had been obtained; such recognition does not exempt the holder of the foreign qualification from complying with any other conditions for the practice of the profession concerned that may be laid down by the competent governmental or professional authorities in the States concerned".

[4] See <https://en.unesco.org/themes/higher-education/recognition-qualifications/global-convention> accessed 5 October 2019.

[5] See the pilot description on the web-site of the WCO: CADENA, a blockchain enabled solution for the implementation of Mutual Recognition Arrangements/Agreements, by Sandra Corcuera Santamaria, Inter-American Development Bank, <https://mag.wcoomd.org/magazine/wco-news-87/cadena-a-blockchain-enabled-solution-for-the-implementation-of-mutual-recognition-arrangements-agreements/> accessed 16 November 2019.

[6] See Contxto, "Brazil wants to build customs connectivity with blockchain", by Mariana López, <https://www.contxto.com/en/brazil/brazil-build-customs-connectivity-blockchain/>, and mic news, "Brazil to trial blockchain for customs", <https://www.mic-cust.com/insights/posts/detail/ad/brazil-to-trial-blockchain-for-customs/> both accessed 12 January 2020.

[7] See lapatilla, "Países de Mercosur conectan sus sistemas aduaneros a través de una blockchain", <https://www.lapatilla.com/2020/11/05/paises-de-mercosur-conectan-sus-sistemas-aduaneros-a-traves-de-una-blockchain/> accessed 10 November 2020.

[8] See IBM web-site: Maersk and IBM Introduce TradeLens Blockchain Shipping Solution Industry-wide collaboration announced in January advances as more than 90 organizations participate in the global trade solution, Copenhagen and Armonk, N.Y., Aug. 9, 2018, <https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution> accessed 11 November 2019.

[9] See web-site of the WCO: TradeLens uses blockchain to help Customs authorities facilitate trade and increase compliance, by Stewart Jeacocke, Global Customs Expert, IBM, and Norbert Kouwenhoven, TradeLens Authorities Lead, IBM, <https://mag.wcoomd.org/magazine/wco-news-87/tradelens/> accessed 16 November 2019.

government procurement – which were developed mainly for domestic purposes, but may be used also on a transborder basis. One running e-procurement application in a developing country is the Chilean platform *ChileCompra*.[10] Also Thailand announced an e-procurement project.[11] The Report on "Blockchain: a forward-looking trade policy" (European Parliament, 2018) stated that "there are at least 202 government blockchain initiatives in 45 countries around the world and economies in regions of Asia-Pacific, the Americas and the Middle East, in particular, are investing in blockchain technologies for trade",[12] of which numerous examples are provided by Emmanuelle Ganne in WTO (2018).

1.3. Perspectives and driving forces for platformisation of transborder recognition procedures

The author believes that an interest for "transnational digitisation", i.e. transnational DLT-enabled projects with the participation of government authorities, will grow. This will be facilitated by the technical work done under the auspices of the International Telecommunication Union (ITU) especially in terms of standardisation on all aspects of DLT. A most welcome example is the recent ITU (2019) set of definitions of DLT-related terms agreed in this universal organisation. Compared to the previous "jungle" of proposed definitions, the ITU document has the advantage of proposing (at a relatively high level of abstraction) a common ground that will allow participants in multi-stakeholder intergovernmental projects to mean and understand the same thing when they use the same term. The present paper relies exclusively on the definitions of ITU (2019).

In respect of education, the benefits of digitation have been realised by some ministries and single educational institutes as suggested by the few initiatives to create "digital diplomas" or "certified electronic diplomas" (CeDiploma) (see Section 4.1). The concept of qualification in recognition procedures is broader than just diplomas (see Section 3.1), and usually would encompass vocational training, professional experience and licenses. However, a large part of recognition decisions relate to diplomas.

Recently, convincing initiatives regarding the digital IDs (DIDs) and self-sovereign identities (SSI) have emerged. One prominent example is Sofrin.[13] The Decentralized Identity Foundation (DIF) is also known for "developing the foundational elements necessary to establish an open ecosystem for decentralized identity".[14]

The aforesaid developments open fresh perspectives in relation to procedures for official recognition of diplomas and other proofs of qualification. For example, a degree-holder could create a controllable sovereign digital identity, and append to it any verifiable educational credentials. This is called the "distributed identity". This set of data could then directly flow into any administrative procedures, including at transnational level.

In respect of the right to privacy, a few Data Protection Authorities (DPAs) made thorough examinations of blockchain. Two reports were published simultaneously late 2018 by the French CNIL (2018) (Commission Nationale de l'Informatique et des Libertés) and the European Union Blockchain Observatory and Forum (2018). Whilst the DLT do raise privacy issues, they are already identified and both developers and authorities are working on them.

Recognition of foreign qualification intrinsically implies some degree of international cooperation between government agencies. That fact, compounded with the above technical developments, is a strong rationale for examining options for migrating the hitherto conventionally administered procedures into a digital platform involving several states participating to it on equal footing. That would amount to a platformisation of e-recognition. In their article on that concept, Poell, Nieborg and van Dijck (2019) define platformisation namely "as the penetration of infrastructures, economic processes and governmental framework of digital platforms in different economic sectors and spheres of life" (emphasis added).

However, the recognition community has not (yet) experienced a transformative change of its operational model.

1.4. Research objectives

The aim of this article is to explore what are the factors and parameters that could support or hinder the use of blockchain technologies in this field of international relations. This article seeks to investigate the potential opportunities that DLT offer, technical options that are available in developing and configuring a DLT-enabled project, and the challenges that may arise in implementing a DLT-based system of recognition. This article doesn't aim to offer a standard recipe on implementing a DLT solution for recognition procedure, nor to state whether such solution is a valid idea, for two reasons. First, this would depend on each country's circumstances, such as available resources, political priorities, administrative practice, the number of domestic authorities involved, systems and tools already adopted, the problem (s) to be fixed if any, regulation of professions, international cooperation practice, average number of recognition procedures, and last but not least stakeholders' preferences. Second, technology improves so fast, and probably exponentially, that any too specific conclusions drawn at the time of researching this topic may be partly outdated at the time the published article will be read.

That said, the research questions that this piece attempts to address are:

- Is there a scope for the use of DLT and in particular blockchain tools in recognition processes?
- What are the opportunities thereof?
- What are their challenges?
- What developments are needed to facilitate their adoption?

Those questions are addressed in Sections 5 and 7 of this article, while Section 6 offers a concrete example of configuration of a blockchain-based e-recognition platform.

2. The global economy and transborder recognition of qualifications

The demand for recognition of foreign qualifications is on the rise worldwide. This is spurred by the sharp increase of transborder technology-mediated work at a distance illustrated by the supply of e-health services and solutions, the growing international trade in services, and other new opportunities opened by globalisation. Before globalisation, recognition of qualification was almost exclusively a North-North issue, mainly between neighbouring countries. Then the number of applicants from developing countries grew steadily. An interesting phenomenon is that with the economic growth of some developing countries the demand for recognition of diplomas, including in respect of applicants from "rich" developed countries, is increasing in some parts of the southern hemisphere. This reverse recognition pattern might partly be explained by a tendency of migrant families in the north to relocate to their respective countries of origin. The day may come when recognition will be significant in south-south relations too, but unfortunately no research is being conducted in that respect.

[10] See "Dirección ChileCompra" at <https://www.chilecompra.cl/> accessed 10 November 2019.

[11] Ledger Insights – Enterprise blockchain news, November 2019, "Thai government to use blockchain for VAT refunds, bonds, procurement" <https://www.ledgerinsights.com/thai-government-blockchain-vat-bonds-procurement/> accessed 16 November 2019.

[12] "Report on Blockchain: a forward-looking trade policy" (2018/2085(INI)), Committee on International Trade, A8-0407/2018, 27.11.2018, <http://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.html> accessed 10 October 2019.

[13] See <https://sovrin.org> accessed 3 December 2019.

[14] See <https://identity.foundation/#home> accessed 3 December 2019.

Recognition of foreign professional qualifications is more often than not connected with mobility (or movement) of persons, whether temporary or permanent. The main types of mobility are outright migration (change or domicile, permanent resettlement), and movement of persons in the context of the supply of a service. The latter case is very common for professional services where a natural person of a country needs to travel temporarily to fulfil a services contract with a company in another country. Engineers sent abroad for a few days to repair an industrial equipment, hospital equipment or an elevator may be requested a valid qualification recognised by the competent recognition authority of the country of destination.

In addition to the motives for recognition that derive from a movement of natural person strictly speaking, there are some other situations that make recognition a necessity. IT-enabled cross-border supply is technically possible in an increasing number of services sectors, some of them being heavily regulated in the importing country. It may happen that regulatory measures that request the supplier of a given service to have a specific degree or qualification are applicable also to a person residing abroad and working online. In such a case, the client (e.g. the buyer of an architectural design) must ensure that the service supplier with foreign qualifications has fulfilled any recognition requirements of the importing jurisdiction. The General Agreement on Trade in Services (GATS) has defined four such “modes of supply” in services trade.[15] However useful the conceptual distinction between modes of supply, the supply of a service by a natural person to a client abroad would often involve both transborder supply and some travelling. For example, though an architect or civil engineer (whether self-employed or employed by a company) could do most of the desk work and send the designs without having to travel, at some point of the execution of the construction project an on-site visit would be indispensable. In terms of business models and practices, both modes of delivery are often impossible to disentangle. The concept of "modes of supplied" as defined in the GATS are useful to categorise legal commitments by Members and to negociate them. However in actual business models there are no so strict boundaries. One example relates to remote IT supported technical works, where a technician sent abroad to repair an industrial equipment is connected to and executes in real time machine or human generated instructions. Similarly, large scale software maintenance is nowdays routinelly a combination in real time of movement of a natural person and connected remote assistance or computer programmes. In terms of verifying the qualifications, it becomes meaningless to attempt to determine if an operation was performed either by the natural person present or remotely: it is both at the same time.

Another mode of exporting services is by setting up a company, a subsidiary or a branch in the importing country. In that case any pieces of domestic legislation requesting the manager or other key personnel to have a particular degree would apply (e.g. the director of a foreign hospital, the director of a foreign school, the chief accountant of a foreign bank or auditing firm).

In all those cases, whenever a profession is regulated, and in any case when specific competence levels are required, the degree holder would need to apply for the recognition of qualification with the competent recognition authority of that jurisdiction.[16]

An example of list of regulated professions and competent regulatory authorities is found for the EU in the EU Single Market “Regulatory professions database”.[17]

To illustrate more concretely the relevance of recognition and its trade-facilitation dimension, the case of installers and maintainers of industrial machinery and equipment is a good example.[18] When a manufacturer of industrial machines sells an equipment, the contract contains an obligation for the manufacturer to install the equipment and ensure regular maintenance and emergency repairs over a long period of time. A failure to deliver would trigger heavy penalties. Given the high specialisation of the workforce (who often is trained for that specific type of equipment), it would be too costly to have a team of installers and maintainers in each export market, especially if the manufacturer exports on a worldwide basis. Rather, the team of technicians would fly in either from the headquarter or from a regional hub. Whilst installation may be planned in advance, and may involve a relatively extended period of stay, emergency repair is unpredictable, requires immediate action on-site and involve only a short stay. In many countries, migration rules accommodate the special needs of that type of service provision. However, in case the service to be supplied falls into the scope of a profession that is regulated, the competent recognition authority would want to verify the qualifications and credentials of each team member. Whether the team is sent over for an installation, a regular (scheduled) maintenance or an emergency repair, smooth and predictable recognition procedures would facilitate the movement of installers and thus international trade in machinery and equipment.

3. State of play in recognition of foreign qualifications

3.1. Scope and methods of recognition of foreign qualifications

Most jurisdictions have a recognition practice, and in most cases it distinguishes academic and professional recognition, with differences in terms of procedure, organisation, content and of course legal effect. Academic recognition – which is not the topic of this paper – determines whether a particular foreign degree is accepted for the purpose of admission in a university (students’ mobility) and thus concerns mainly educational institutions. Professional recognition – the topic of this paper – concerns the regulatory authorities and has a relevance only for occupations that are regulated and are subject to professional competence requirements (professional mobility). Unlike academic recognition, professional recognition covers all types of proof of qualification such as university degrees, vocational and technical training, experience, licenses, registration requirement, depending on the specificities of each jurisdiction’s regulatory framework. This is why this article often uses the expression “international mobility of skills” or “international trade inof skills” .

There are a few other differences between academic and professional recognition. Professional recognition is granted to the individual applicant in the form of a decision by the authority, not only in the context of autonomous recognition practice but at times even when recognition is based on a mutual recognition agreement (MRA) (see below). By contrast, academic recognition refers in general to the mere fact that universities, respectively their degrees, are recognised for admission by applicants in universities abroad; the individual foreign student doesn’t apply for recognition and doesn’t receive a recognition decision. Consequently, in academic recognition (unlike professional recognition) there is no room and need for recognition application by a third party (e.g. the employer) on behalf of the degree-holder; there is no such situation as the denial of a recognition application; and there is no room for counterfeit recognition decisions.

More crucially academic recognition has no bearing on the market, i.e. on the quality of the service received from practitioners by consumers, patients, etc. To illustrate those differences from a concrete

[15] The four modes of supply are set out in Article I:2 of the GATS.

[16] The term “competent recognition authority” is defined by the UNESCO Global Convention as “an entity which, in accordance with the laws, regulations, policies, or practices of a State Party, assesses qualifications and/or makes decisions on the recognition of qualifications.”

[17] See “EU Single Market – Regulatory professions database” at <https://ec.europa.eu/growth/tools-databases/regprof/index.cfm?action=homepage> accessed 10 November 2019.

[18] For a description of the services provided by installers and maintainers, see “Communication from Switzerland – Temporary Admission of Installers and Maintainers under the GATS: A Case for Mode 4 Commitments”, World Trade Organization document TN/S/W/61, 2 April 2007, (07-1344).

angle, a country may admit in doctorate programmes students with a particular foreign master's degree, however, if such foreign degree-holder wants to exercise the profession (assuming that at least a national master's degree is required for practice) not only a formal application for recognition would be needed but it may well be that it could be denied if the level of professional qualification is not deemed exactly equivalent to national master's degrees. Conversely, in particular if the profession is not regulated, a degree-holder from some foreign university would be allowed to work but would not be admitted for higher-level study in the discipline at stake. These differences have an impact on the options for DLT applications in those two fields, their opportunities and challenges, and crucially on who are the stakeholders involved and on their interests.

There are two modalities of state recognition of foreign qualifications for the purpose of the exercise of a regulated profession: the autonomous one and the treaty-based one. The former is much more widespread than the latter. The latter typically takes the form of MRAs, to which this article now turns.

3.2. Mutual recognition agreements (MRAs)

The term "mutual recognition agreement" and its acronym MRA are used in several fields of international relations. Thus, it is helpful to propose a difinition of this term that suits the specific context addressed in this article:

MRAs are legally-binding international instruments setting out procedures to facilitate the recognition of professional qualifications obtained in the parties to such instrument. They usually focus on a specific, pre-established list of qualifications and educational institutions and are concluded mostly at bilateral, sometimes at plurilateral, level. Natural persons who hold a degree or other credential listed in the MRA would normally have access to the corresponding regulated profession without having to apply for an individual recognition decision.

One example of a bilateral agreement on mutual recognition of professional qualifications is the "Arrangement Relating to Trans-Tasman Mutual Recognition" (commonly called Trans-Tasman Mutual Recognition Agreement, TTMRA) between Australian Parties and New Zealand, signed in 1996, which covers both goods and professional occupations. The definition of "occupation" under the TTMRA is illustrative of the typical scope of recognition:

"Occupation means an occupation, trade, profession or calling of any kind that may be carried on only by Registered persons, where Registration is wholly or partly dependent on the attainment or possession of some qualification (for example, training, education, examination experience, character or being fit or proper), and includes a specialisation in any of the above in which Registration may be Granted".[19]

3.3. International recognition frameworks

Whilst both avenues, autonomous or trough an MRA, prove useful for individuals seeking to exercise a regulated profession in a particular foreign jurisdiction, none would make it possible for people to have their qualifications accepted on an international basis. This is why broader schemes are sometimes needed. Some professions may be covered by an international framework that facilitates recognition, either at intergovernmental or private level. One example of intergovernmental framework is under the auspices of the International Maritime Organization (IMO), namely regulation I/10, paragraph 1.2 of the Annex to the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978, as amended, (hereinafter referred to as the "STCW Convention") and Section A-I/10 of the Seafarers' Training, Certification and Watchkeeping Code (hereinafter referred to as the "STCW Code").[20] The Convention and Code establish common basic requirements and minimum standards of competence required for seagoing personnel and set out procedures to periodically produce a list of confirmed Parties (i.e. countries) that comply with the STCW Convention. This provides a framework for STCW Parties to bilaterally recognise other Parties' certificates for service on ships flying their flag in a consistent and harmonised manner.

One example of private scheme is the international certification for welders granted by the International Institute of Welding (IIW).[21] IIW has developed a harmonised qualification and certification system for personnel in various welding specialities and at all levels of qualification. Certificates awarded are recognised among all members. According to the EU, welders rank sixth in terms of temporary mobility, before medical doctors and architects.[22]

3.4. The UNESCO Global Convention on the Recognition of Higher Education Qualifications

As mentioned, the UNESCO Global Convention was opened for signature in September 2019. This legally binding international treaty builds on decades of incremental work on recognition done under the auspices of UNESCO, in particular the 1993 *Recommendation on the Recognition of Studies and Qualifications in Higher Education*,[23] and a series of subsequent regional and inter-regional normative instruments in this field. It also builds on the Council of Europe Convention on the Recognition of Qualifications concerning Higher Education in the European Region of 1997 (better known as "Lisbon Recognition Convention").[24] Given these pre-existing regulatory frameworks, the negotiation of the Global Convention was relatively short and smooth. The aims of the Global Convention are broad, but essentially the purpose is to extend on a global scale the level of academic mobility that had been reached at regional levels. In particular, agreed principles for recognition of higher education are now established at global level. As will be underscored *passim* in this article, the focus of the Global Convention is very much on academic recognition and only marginally on official recognition of regulated professionals.

3.5. The GATS and international trade agreements

The General Agreement on Trade in Services (GATS) is one of the agreements resulting from the Uruguay Round of negotiations and formally is an annex to the WTO Agreement (World Trade Organization). The main aim of the GATS is for its Member States to undertake commitments on national treatment and market access for services and service suppliers from other Members, but it also contains in its Article

[19] See also New Zealand Foreign Affairs and Trade, "Recognising New Zealand qualifications" at <https://www.mfat.govt.nz/en/countries-and-regions/australia/new-zealand-high-commission/living-in-australia/moving-to-australia/recognising-new-zealand-qualifications/> accessed 14 November 2019. The TTMRA was considered as a "logical extension" of the Australia New Zealand Closer Economic Relations Trade Agreement (ANZCERTA).

[20] Available at <http://www.imo.org/en/OurWork/HumanElement/TrainingCertification/Pages/STCW-Convention.aspx>; see also <http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-on-Standards-of-Training,-Certification-and-Watchkeeping-for-Seafarers-(STCW).aspx> accessed 20 October 2019.

[21] See <http://iiwelding.org/qualification-certification>, in particular "IIW-IAB Education, Training and Qualification System for Welding (and related technologies) Personnel" <https://www.ewf.be/home_iiw/qualificationiiw-iab.aspx> and IIW-IAB Personnel Certification Scheme <https://www.ewf.be/home_iiw/certificationiiw-iab/iiw-iab-personnel.aspx> accessed 20 October 2019.

[22] See the EU Single Market "Regulated professions database", Ranking for temporary mobility (EU/EEA and Switzerland) <https://ec.europa.eu/growth/tools-databases/regprof/index.cfm?action=stat_ranking&b_services=true> accessed 20 October 2019.

[23] Available at: <http://portal.unesco.org/en/ev.php-URL_ID=13142&URL_DO=DO_TOPIC&URL_SECTION=201.html> accessed 20 October 2019.

[24] Available at: <https://rm.coe.int/168007f2c7> accessed 20 October 2019.

VII a clause on Recognition.[25] The main rationale of this clause is to provide an assurance that in spite of the strong most-favoured-nation obligation (MFN) set out in GATS Article II, recognition could not be seen as a breach of the GATS. Accordingly, the main provision of this clause is that Members "may recognize the education or experience obtained, requirements met, or licenses or certifications granted in a particular country" whether autonomously or treaty-based. The term *country*, in contrast to *Member*, refers to any country in the world, which confirms that this provision is primarily a safeguard of national recognition schemes against the MFN obligation (rather than a soft recognition obligation vis-à-vis other GATS Members).

To avoid abuses of this safeguard for protectionist purposes, paragraph 3 of Article VII adds that Members "shall not accord recognition in a manner which would constitute a means of discrimination between countries in the application of its standards or criteria for the authorization, licensing or certification of services suppliers, or a disguised restriction on trade in services".

However, given the central role of the MFN principle in trade law and its vital importance for most WTO Members, the provision goes further than that and states that Members that have recognition instruments "shall afford adequate opportunity for other interested Members to negotiate their accession" to such instruments. This refers mainly to MRAs (see definition above).

Article VII of the GATS is replicated in most Free Trade Agreements (FTAs) and regional trade agreements (RTAs). Some countries which are particularly ambitious in respect of recognition of professionals use to reinforce the original GATS provision, typically by including in their agreements a dedicated annex setting out good practices in recognition procedures. For example, bilateral disciplines pertaining to recognition are found in Annex 4-III of the Singapore-Australia Free Trade Agreement (SAFTA).[26]

Official recognition is available to any individuals irrespective of the type of mobility at stake. By contrast, because the scope of the GATS is limited "to measures by Members affecting trade in services" (GATS Article I), any of its provisions are applicable only to measures pertaining to natural or juridical persons in the realm of trade in services. In particular, the concept of movement of natural persons, when limited to its trade-related component, is defined as the supply of a service "by a service supplier of one Member, through the presence of natural persons of a Member in the territory of any other Member" (GATS Article I:2(d)). This is also called GATS "mode 4".

Commitments undertaken by Members under the GATS would bind their regulatory measures only inasmuch as these measures fall within the scope and definitions of the Agreement. In that sense, the term *trade in services* is narrower than *supply of services*, labour mobility, mobility of skills or trade in skills. For example, taking a fictive "country A", while the transfer by a foreign multinational company of a highly qualified engineer from a branch abroad to its branch in country A would be captured by GATS commitments of country A, the same sort of intra-corporate transfer by a domestic multinational corporation would not. Natural persons simply entering the labour market of a foreign country do not fall within the scope of GATS either, even if they work in the services sector and are foreigners, as this is more an issue of labour mobility than international trade in services as defined in the GATS.

Transborder tourist guides' services are another case that illustrates the differences between the above concepts and definitions. Many jurisdictions impose qualification requirements on tourist guides (sufficient cultural, historical and linguistic knowledge), and foreign tourist guides would have to apply for recognition of their home country qualifications. Provided they affect trade, e.g. because of some *de jure* or *de facto discriminatory effect*, such measures would fall within the scope of the GATS. However, measures affecting a guide from country A who would simply work for a tour operator in country B for the summer holiday season would not be covered by the GATS. A tour operator of country B sending to country A a group of tourists including their own tourist guide would not be captured either. The reason is that none of those activities are captured by any of the four modes of supply as set out in Article I:2 of the GATS. Yet another example would a pharmaceutical company sending one of its doctors to a third country to supervise a clinical trial that the company is making there.

In the case of bilateral trade agreements, say between country A and country B, an exact transposition of the aforementioned GATS mode 4 definition means that, for example, a service company of country A supplying in the territory of country B a service through the presence of a person who is not a national of either A or B would not be captured by the agreement.

Taking the case of Switzerland, the bulk of recognition decisions (and entry permits) do not relate to natural persons who would fall within the scope of the GATS. This does not diminish however the central importance of this multilateral agreement for trade-related movement of natural persons.

3.6. State accreditation

One key feature of professional and academic recognition of foreign degrees that needs to be underscored is that the vast majority of recognition policies apply only to degrees accredited under a state accreditation system, i.e. degrees granted by state institutions, excluding for example private universities. A programme that a state-accredited university offers outside the realm of its accreditation, so to say on a private basis, would often not be considered for recognition. This policy of focusing on state accreditation is either an explicit one, or it is simply implemented so in practice.

This state-centred approach of recognition policies is well reflected in the UNESCO Global Convention, notably in the following definitions:[27]

"Higher-education institution: an establishment providing higher education and recognized by a competent authority of a State Party, or of a constituent unit thereof, as belonging to its higher-education system" (emphasis added)

and

"Higher-education programme: a post-secondary programme of study recognized by the competent authority of a State Party, or of a constituent unit thereof, as belonging to its higher-education system and the successful completion of which provides the student with a higher-education qualification" (emphasis added)

The term "recognized" in the two definitions does not refer to recognition of *foreign* degrees but to the *domestic* accreditation of a school or programme within the national education system. It means that the degree granted by a school or a programme falls into the scope of application of the Global Convention only if that school or programme is accredited with the national competent education authority (e.g. ministry).

In the context of an article that considers the relevance of blockchain in recognition, this feature needs to be kept in mind. This is because, when it comes to higher academic degrees, most countries' recognition systems follow the same lines as in the UNESCO example.

[25] Available at: <https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleVII>.

[26] More specifically its Section 1 "Recognition of law degrees for admission as qualified lawyers" <https://www.enterprisesg.gov.sg/-/media/esg/files/non-financial-assistance/for-companies/free-trade-agreements/Singapore-Australia-FTA/Legal-text/Chapter-7/Annex-4-III-Additional-Commitments> accessed 14 November 2019.

[27] As underscored in Section 3.4, the UNESCO Global Convention is dedicated mainly to so-called academic recognition, i.e. recognition for the purpose of being admitted for studies in a university abroad. The Convention does also cover recognition for the purpose of exercising a profession in another jurisdiction, the topic of this paper, but only to a limited extent.

This boundary between what may be subject to official recognition and what is outside the realm or recognition is not always straightforward to implement. In the case of the Swiss experience – one of the countries having a policy of recognition strictly limited to state-accredited qualifications – the question of determining whether a particular foreign degree meets that criteria has sometimes not been easy to solve on the sole basis of the file received from the applicant (see Section 4.2). If so, the authority would seek information from the authority of the other country.

4. Issues in recognition of foreign qualifications

This Section elaborates on two aspects of recognitions that are relevant for investigating a scenario of DLT-based transformation: ensuring trust in the system and exchange of information between authorities.

4.1. The administration of trust

Blockchain has been nicknamed a "trust factory", "trust machine" or "confidence machine". Many authors also simply characterised it as being "trustless".

The first key question to consider when examining the relevance of blockchain in a particular sector is thus whether there is a need for high level of trust. In the case of recognition, the answer is definitely "yes", for several reasons. One is that recognition sometimes applies to very sensitive professions, for example in the health sector. Another reason that will be discussed in details in connection with information exchange (see Section 4.2) and standardisation (see Section 7.1) is the fact that a recognition decision relies on the assessed level and quality of the foreign degree at hand, and thus relies on the trust that the authority is ready to give to the submitted description of the curricula. Yet another reason is that the problem of "fake" certificates of qualification is perceived as a real one. The issue of "fake" credentials is a complex one, as the complexity starts with its definition. As Grolleau, Lakhal, and Mzoughi (2008) recall, "[t]here are no definitive criteria to characterize a fake degree or a diploma mill and the lack of consensus on terms may generate some confusion".

From the outset, in the context of this article the question of "diploma mills" (often considered as one aspect of "fake" diplomas") shall be excluded because the types of recognition considered in this article are normally limited to institutions accredited by a state. Hence, for the purpose of this article, fake certificates will be defined essentially as:

Forged credentials which either (in the most sophisticated cases) exactly counterfeit the genuine credential of a known institution, in particular the paper used, seals and signature, or (in less sophisticated cases) grossly imitate such credential to give the impression that it is an original. Forged credential also include falsification of originals, i.e. the *ex post* unauthorised modification of specific data (e.g. the expiry date of a credential). In addition to diplomas as such, forgery may also concern lists of grades and other related documents. In respect of qualification requirements regarding experience, such types of forgeries apply, *mutatis mutandis*, to work certificates.

For example, in Switzerland recognition in medical professions is granted on the condition (among others) that the applicant successfully attended a course on medical ethics. Thus, in case the ethics course was optional in the foreign curriculum, an applicant may submit a genuine diploma, but a forged document claiming that he attended that course. This example also illustrates why this article prefers to use the term *credential* rather than just *diploma*.

Grolleau, Lakhal, and Mzoughi (2008) have a broader understanding of this term, stating that "[o]ur definition of fake degrees includes both replica testamurs from bona fide institutions and testamurs that can either be bought or earned with little work from an entity of some description". Literature on "fake" certificates usually do not consider fraudulently obtained "original" certificates (see below). Literature also seems to overlook the possibility of "full" fakes, i.e. a document mentioning a non-existing institution.

Grolleau, Lakhal, and Mzoughi (2008) stated that quantification of this phenomenon is very scarce, and this situation has not evolved to date. However among practitioners the necessity to prevent and uncover cases of forgery is regarded as a high priority.

A trust-related issue that is often mentioned in some sectors of public administration such as customs administration or government procurement, seems to be much less relevant in the field of recognition: corruption and fraudulent issuance of "authentic" certificates. But here again, consolidated statistics don't exist and in any case figures would only show the cases that are detected and proven, not those that go unnoticed. Finally, another way to cheat the system is to counterfeit a recognition decision itself. As well, this is rare but not inexistent.[28]

An examination of the notifications made in the European Union's Internal Market Information System (IMI) shows that the number of reported cases of diploma falsification is comparatively low, and reported cases of fraudulently obtained authentic diplomas is almost inexistent.[29] This is only a partial insight, and given the absence of quantitative analysis it is impossible to know whether at the global scale the risk is marginal or systemic. IMI covers all types of falsification of titles and degrees in the context of recognition.[30]

Whatever its magnitude forgery is a perceived problem, so much so that one of the principles of the UNESCO Global Convention is that "States Parties commit to adopting measures to eradicate all forms of fraudulent practices regarding higher education qualifications by encouraging the use of contemporary technologies and networking activities among States Parties".[31] "Networking activities" essential means exchange of information between countries (see Section 4.2).

Thus, a major task of the recognition authority is to ascertain the authenticity and validity of documents submitted by the applicant[32] – concretely the authenticity of signatures. In most countries, the originals are not required in the application process, however a legalisation of the documents or more precisely of certified copies is a must. There are in general two avenues for that purpose.[33] One is through notarisation in the country of origin of the document and authentication by an authority (the ministry of foreign affairs), complemented by consular certification, which amounts to a double authentication by authorities of the originating and the receiving countries. The other is via the procedures of the Hague Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents, in its short form the "Apostille Convention".[34] The procedures under the Apostille Convention are administered by a governmental authority (or several ones concurrently), which may be either the same that has competences for other forms of legalisation or a different one. The Apostille legalisa-

[28] In the past year two such cases were uncovered in Switzerland, both involving European nationals.

[29] IMI, <https://ec.europa.eu/internal_market/imi-net/index_en.htm> accessed 14 November 2019.

[30] The scope of IMI is limited by the scope of its legal basis, Directive 2005/36/CE on the recognition of professional qualifications, OJ L 255/22, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0036> accessed 2 October 2019.

[31] Para. 8 of Article III of the Global Convention.

[32] The term applicant is defined by the UNESCO Global Convention as: "(a) an individual submitting to the competent recognition authority a qualification, partial studies, or prior learning for assessment and/or recognition; or (b) an entity acting with consent on behalf of an individual." Where (b) refers mainly to cases where the application is submitted by the organization employing the degree-holder, for example when an engineering company needs to send a team abroad to perform a service.

[33] The variety of international legalisation practice is presented in Kenneth W. Abbott et al. (2000), "The Concept of Legalization", International Organization, 54(3):401-419.

[34] Convention de La Haye du 5 octobre 1961, entered into force on 24.1.1965. The full text of the Convention and the status report are available at <https://www.hcch.net/en/instruments/conventions/status-table/?cid=41> accessed 14 November 2019.

tion is then accepted by authorities of the country of destination without consular certification (hence, no double authentication).[35]

This needs to be taken into account in a blockchain project. In particular the initiators of such project should decide whether starting the blockchain procedure after the Apostille (or similar) procedure is completed, or whether documents uploaded into the blockchain and validated onchain by the institution that issued them (e.g. a university) could be considered by the recognition authority to be authentic, and thus skip the requirement of notarisation and Apostille.

Until recently, the second possibility would have seemed unrealistic. However, things may change, in particular because education institutions start introducing fully computerised credential issuance and verification systems, many of which are presented in the overviews made in 2017 by the European Commission Joint Research Centre (2017) and more recently by Rodrigues et al. (2020). In the same year as the EU research a general assessment of the potential and perspectives of online verification of the authenticity of educational credentials was already presented by Martin Hall.[36] One example of innovation made at government level is the French digitally certified degrees.[37] This database encompasses all educational levels throught the whole country. One purpose of this application is to allow third parties, such as prospective employers, to verify the authenticity of a given diploma with a quick, costless and personal data secure web application. The Netherlands as well has set up an online register of diplomas.[38] Some individual universities offer their own "certified electronic diploma" (CeDiploma), such as among others the University of St. Gallen, Switzerland.[39] A very recent private platform that relies exclusively on blockchain certification is *BC Diploma*.[40] But this as well remains far from a recognition system. The purpose of this business model seems to be, at this stage, mainly domestic and mainly private, e.g. aimed at potential employers. (Badr et al., 2019) proposed a blockchain-based end-to-end solution but this, as most others, pertains to the academic recognition only as it focuses on the transfer and verification of transcripts, certificates and other academic records between educational institutions as prerequisites for acceptance into academic programs or for credit transfer. In sum, the above tools and proposals are often conceived primarily for domestic purposes and don't always embrace blockchain technologies. They remain far from a full-fledged recognition system, but they represent a valuable innovation facilitating the deployment of e-administration. Besides, to date, they cover mainly credentials that are not relevant for decisions on recognition for the access to regulated professions and do not seem to have any particular focus on transborder access to such professions. Those innovations show, however, that there seems to be a demand for computerised certification of qualifications and that it technically can work.

Taken altogether, the foregoing exemplifies the importance of trust in any recognition process. It thus doesn't come as a surprise if the very first principle mentioned in paragraph 3 of Article III of the Global Convention is trust: "Recognition decisions are based on trust, clear criteria, and fair, transparent and non-discriminatory procedures, and underline the fundamental importance of equitable access to higher education as a public good which may lead to employment opportunities".

4.2. Exchange of information between authorities

Though the confirmation of the authenticity of a foreign document, respectively of the signatures on it, is a fundamental step towards recognition, it is only a first step. The next step is to assess the level of a foreign qualification. For that purpose, the receiving authority must obtain reliable information about curricula, exams, marking, compulsory practical experience and sometimes admission criteria relating to a particular qualification degree.

The central role of access to and exchange of information in a recognition process has been reflected in the UNESCO Global Convention. In terms of its objectives, the Convention states in Article II that:

"Building on and enhancing the coordination, revisions and achievements of the regional recognition conventions, the objectives of this Convention are to:

[…]

Promote the development, collection and sharing of accessible, up-to-date, reliable, transparent and relevant information […]" (emphasis added)

In terms of its principles the Convention states in Article III that:

"For the recognition of qualifications concerning higher education, this Convention establishes the following principles:

[…]

4. Recognition decisions are based on appropriate, reliable, accessible and up-to-date information on higher-education systems, institutions, programmes and quality assurance mechanisms which has been provided through the competent authorities of the States Parties, official national information centres, or similar entities." (emphasis added)

The immediate source of information would be the applicant, who is normally requested to provide those pieces of information together with the application. This well-established principle has been confirmed in paragraph 1 of Article IX of the Global Convention, which states that "[i]n the first instance, the responsibility for providing adequate information rests with the applicant, who shall provide such information in good faith". But more often than not, if the application relates to a qualification not yet known to the receiving authority, the latter would also contact directly the competent authority of the country of origin to complement or double-check the information obtained from the applicant. This is reflected in paragraph 3 of Article IX: "Each State Party shall ensure that the institutions belonging to its education system provide to the extent available, upon request, within a reasonable time frame and free of charge, relevant information to the holder of a qualification or to the institution or the competent recognition authorities of the State Party in which recognition is sought".

While some types of degrees are relatively easy to classify in terms of level, others, for example in the context of continuing education, are not. All in all the amount of information to handle and keep updated is sizeable for a national authority that would receive applications from several regions of the globe. This is where, for example, a system like the IMO's STCW Convention is useful, as it tracks in a centralised manner any changes and implementation practices of training schemes of individual jurisdictions (see Section 3.3).

5. Potential benefits accruing from DLT for foreign qualification recognition

5.1. Framing the approach

The UNESCO Global Convention remains very evasive when it comes to the role of technologies in recognition procedures, which is

[35] In the case of Switzerland, the Hague Apostille is administered by the Federal Chancellery <https://www.bk.admin.ch/bk/en/home/service/legalisations.html>, respectively cantonal chancelleries for cantonal documents. In other countries it may be the ministry of justice. An example of legalisation services of diplomatic representations is found on the web site of some Swiss embassies, such as <https://www.eda.admin.ch/countries/morocco/en/home/services/legalisations/legalisation-official.html> accessed 14 November 2019.

[36] Hall, Martin (2017). *Blockchain and the future of credentialing: Getting ready for smart contracts*, by GetSmarter, April 2017.

[37] See "La plateforme d'attestation des diplômes du Ministère de l'Education nationale et de la Jeunesse et du Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation" at <https://diplome.gouv.fr/sanddiplome/login> accessed 14 November 2019.

[38] See "Diplomaregister – Digitaal diploma" at <https://duo.nl/diplomaregister/> accessed 18 December 2019.

[39] ICO.li news, "University of St. Gallen Launches Blockchain-based Diploma Verification System", by Lukas Hofer, 24 September 2019, <https://www.ico.li/university-blockchain-degree-verification/> accessed 1 November 2019.

[40] Vincent Langard, BCD Report #12, 30 May 2020, <https://medium.com/bcdiploma/bcd-report-12-may-30th-2020-44959f789025> accessed 27 June 2020.

understandable given the universal membership of the organisation, which includes countries that are on the wrong side of the digital divide. Besides the specific paragraph on fraud quoted in Section 4.1 above, all what the Convention states is that "[e]ach State Party shall encourage the use of technologies to ensure easy access to information".[41] But before embarking into the characteristic of the technology, it is appropriate to recall some caveat regarding the digital divide and the situation of developing countries.

The difficulty for developing countries and especially Least Developed Countries to overcome the digital gap should not be underestimated. The recent review article by Twizeyimana and Andersson (2019) concludes that "[n]owadays, in contrast to developed countries where e-government is well-established, there are many challenges for e-government in the Least-developed countries (LDCs). These challenges include, but are not limited to, a large digital divide, inadequate e-infrastructure and a lack of skills and competencies for design, implementation, use and management of e-government systems". Mavilia and Pisani (2019) concur by stating that "[blockchain] applications are still at an early stage in developing countries, particularly in Africa". Hence, migrating the recognition systems into a DLT-based platform would represent a challenge for them.

Even though some countries have extensive e-administration systems that also include some components of recognition processes, to date no project exists at national level to migrate a recognition procedure onto a DLT system.

DLT encompass various systems using distributed ledgers, and blockchain is one possible form of data storage in distributed ledgers. Mavilia and Pisani (2019) confirm that there is no "unanimously accepted definition of blockchain"; in fact, blockchain technologies are diverse which makes it difficult to find one set of fully exclusive and fully relevant detailed characteristics. To gather some consensus a definition is bound to remain general, which is the approach chosen by the ITU (2019) in proposing the following definition for DLT:

"Distributed ledger technologies (DLTs), the most prominent implementation of which is Blockchain, enables large groups of nodes in the distributed ledger networks to reach agreement and record information without the need for a central authority".

DLT is just a particular type of technology and as such it essentially allows to implement some processes in a different manner, no more than that. Recognition processes could be made more efficient merely using conventional database technologies and implementing them in a more transparent manner (like open-access). Thus, why opt for a blockchain technology rather than more conventional ones? The reason why that technology should deserve some scrutiny it that it offers not only one, but several advantages that are most relevant in the administration of recognition processes. These are namely trust, information exchange (transaction), transparency, and traceability. They could be coined the "four Ts".[42]

From an e-government perspective the first step in addressing the above question is to identify an element of value transfer resulting from deploying that particular technology.[43] According to Panagiotopoulos, Klievink and Cordella (2019) a value-centred approach, instead of mere efficiency maximisation in the administration, "provides a more encompassing view to account for the complex transformations required to shift the focus from service production to the fulfilment of public expectations and goals". This in spite of the fact that in many respects "there is lack of theoretical clarity on what public value means and on how digital technologies can contribute to its creation", as they noted. For that purpose, a thorough stakeholders' analysis is needed, including an identification of all stakeholders, their interests, expectations and needs, such as the "stakeholder benefits analysis tool" proposed in Rowley (2011). To find acceptance e-administration solutions should provide public value and citizens satisfaction, not just a more efficient bureaucracy. This approach is essential because research suggests that the use of ICTs for e-administration often fails to generate public value and citizens satisfaction, as discussed in Bonina and Cordella (2009) and in Castelnovo (2013). In Scott et al.'s (2016) paper a number of customers values were singled out and analysed in relation to e-government: Efficiency, Effectiveness, Social value, Cost, Time, Convenience, Personalisation, Communication, Ease of Information Retrieval, Trust, Well-Informedness and Participate in Decision-Making.

However, stakeholders and stakeholders' interests would differ from country to country so that conclusions obtained in one setting are not necessarily transferable into another setting. In general, it may be assumed that the main stakeholders in a blockchain project for procedures of recognition of professional competencies would include:

- the client, i.e. the prospective applicants (a key stakeholder group but one that is difficult to reach out to, but may be represented by international professional federations),
- the competent recognition authority of the receiving country, including the staff in charge of administering the procedure,
- other competent authorities in the receiving country interested in recognition, e.g. migration and labour market authorities, sectoral regulatory authorities in the health, education and other sectors,
- the authorities of the countries of origin of applicants,
- recognition authorities from third countries,
- professional associations in the receiving country,
- professional associations in the country of origin,
- employers in the receiving country,
- educational institutions in the receiving country,
- educational institutions in the country of origin,
- the general public (e.g. patients' organisations),
- other regulators of the receiving country interested to be consulted on the design of the system during the development phase (e.g. Data Protection Authority, State archive administration, ICT safety administration).

It may safely be assumed that in most countries the main stakeholders are the four first categories above, and that the interests of the other stakeholders are confined to having transparent access to information (see Section 6.2), and for some of them to ensuring that fraud and mistakes are kept to a minimum. But of course, a more detailed elaboration of stakeholders' analysis can only be performed on a country-specific basis. The problem in the context of a paper that considers an issue that concerns both north and south is the research gap in that respect. In their review article Twizeyimana and Andersson (2019) conclude that "[r]egarding the current state of research on the public value this study found a lack of research on the public value of e-government, especially, in the context of developing countries – and more importantly – a total absence of this kind of research in the Least Developed Countries (LDCs)".

Another feature of the above group of stakeholders relates to the main purpose of DLT. DLT is portrayed as most relevant for decentralised communities of participants where ensuring trust is a major objective. In effect, most stakeholders do see value in improved trust.

In answering the question "Why choose a DLT?" the starting point should be to identify the problem to be fixed, or the improvement to be reached, and find out what is or are the best way(s) for that purpose. In order to minimise the risk of failure of the project, in particular lack of acceptance by stakeholders, it is important to take a "need-driven" approach, as pleaded by Ølnes et al. (2017), rather than a "technology-driven" approach. In other words, it would be wrong to choose blockchain just for the sake of it and because it *prima facie*

[41] Para. 4 of Article VIII of the Global Convention.

[42] The fact that those four characteristics start with the letter "t" is a mere coincidence though. The terms used happen to be those ones quite consistently in the literature.

[43] Value is not only monetary value but also anything that can be monetised. From the perspective of an important group of stakeholders, the certified professionals, value would be enhanced professional reputation and trust that can be monetised.

offers new and interesting features. The EU Blockchain Observatory and Forum (2018) recommended as a "rule of thumb" that launchers of blockchain projects should "[s]tart with the big picture: how is user value created, how is data used and do you really need blockchain".[44]

Sections 5.2 to 5.7 below provide a closer focus on the generally accepted opportunities of blockchain technologies.

5.2. Trust

As set forth in Section 4.1 the benefit of DLT that most obviously comes into mind relates to building trust. This means that recognition authorities would have an alternative to the legalisation of foreign documents and to the Apostille Convention. Applicants would save the costs of legalisation.

Depending on the consensus mechanism or algorithm, the strength of the trust enabled by DLT is high because this technology is considered as very difficult to hack – a dataset, once stored, is immutable and virtually impossible to tamper with and counterfeit. The term "immutable" in DLT terminology is an important one and is defined very precisely. According to the ITU (2019) it refers to the "property of blockchain and distributed ledger systems that ledger records can only be added, but not removed or modified, and are designed not to allow changes to historical data over time".[45] Besides, certain advantages arising from the "non-reputability" of distributed ledgers were highlighted by (Warkentin & Orgeron, 2020).

Another reason why DLT are perceived as trustable is that they are rather robust against bugs and that since the data is stored in a decentralised manner it cannot get lost. Even if one server is entirely destroyed, a copy of the data will always be retrievable somewhere else. Those "safety by design" features are correlated with the number of nodes and participants: with more nodes the system will be more robust, with few nodes (e.g. small private systems) the system may be not much safer than conventional ones. Some caution is warranted here, in view of Conte de Leon et al.'s (2017) warning that "[c]urrently, many websites, books, professional reports and news and academic articles state that blockchains are immutable or unchangeable, and that transactions in a blockchain cannot be modified. As written, these statements are incorrect and misleading".

However, the scope and coverage of the trust provided by a blockchain solution is limited because it relates only to the onchain world, which may sometimes be rather poorly connected with the real world. Helliar et al. (2020) rightly raised the question as to "what about processes that occur before being added to a block?". It must be stressed that the implementation of such technology doesn't help address offchain issues including the difficulty of migrating offchain (real world) data reliably and accurately into the chain. If a degree-holder has obtained the proof of qualification through cheating, collusion or bribery the technology will not help, or worse, it helps carry the fraudulent proof into the system. For that sort of situations face-to-face meetings and human common sense are better ways to build trust, respectively detect causes for mistrust.

This systemic problem with "real world" or "physical world" data migration is not unique to recognition. It was long identified as an issue in blockchain applications in customs and supply chain management (SCM). As Kopyto et al. (2020) put is, "[t]he study further identifies data availability and data authenticity as two major SCM-specific barriers that could prevent the exploitation of potential benefits. These barriers indicate that two of blockchain's promising advantages – namely manipulation safety and negligibility of trust – are not entirely transferable to SCM […] as the authenticity of data entered into a blockchain cannot be guaranteed". Against this background, Helliar et al.'s (2020) finding that "off-chain processes are not discussed enough in the literature" is absolutely to the point.

Moreover, it would be misleading to approach trust and confidence issues are purely technical ones. As De Filippi, Mannan and Reijers (2020) noted in their piece entirely dedicated to those concepts, "[c]onfidence in a procedural system such as a blockchain ultimately depends on the proper governance of that system. This means that the increased confidence derived from the use of blockchain technology is inherently correlated with the degree to which the various actors involved in the governance of the underlying blockchain infrastructure can be trusted to act as expected". Well, if applicants are ready to cheat in the real world, would they refrain from cheating in a blockchain too?

In government administration, trust issues that may need to be fixed or improved may be of a variety of types. Before choosing new tools, including a possible DLT solution, the exact nature of the trust issue at stake needs to be analysed and confronted with the features of the tool contemplated, taking into consideration the configuration of implementation of the case at hand (see Section 6). A risk analysis that states precisely what risks the particular recognition authority wants to control should be an integral part in the management of a blockchain project.

Trust means not only trust between participants but also trust in the system itself. The fundamental aspect of trust in any system is the right to privacy. This is why this article will make numerous references to a feature of DLT called hashing. The ITU defines hashing as "a method of calculating a relatively unique output (called a hash digest) for an input of nearly any size (a file, text, image, etc.). The smallest change of input, even a single bit, will result in a completely different output digest".[46] Concretely, through hashing a diploma would be translated into a string of bits of a fixed length. Applying the hash function to the same diploma several times will always result in exactly the same string of bits. However, the slightest change in the document will result in a different hash digest. Importantly in the context of this article, if two authorities in two countries obtain the same "hash" of the diploma they have before them, comparing only the hashes obtained will give them certainty that the diploma is identical on both sides. The hash function is considered to be "impossible" to crack, i.e. the hash alone cannot be used to know the content of the diploma.[47] In this article, in line with literature, we use the short form "hash" for ITU's "hash digest". To conclude on privacy, a blockchain application that would consist in storing only the hashes may probably be regarded as conferring the highest level of privacy.

5.3. Information exchange and management (transaction)

As explained in Section 4.2 exchange of information between authorities represent an important component of a recognition process, in particular when a hitherto unknown qualification is submitted for recognition. Authorities also crucially need to be kept updated about foreign education systems. DLT are flexible technologies that allow participants to request and exchange information with one another. In a sense, information requests may be more efficiently handled in a blockchain platform compared to conventional electronic mail because the history of the transaction,[48] i.e. the previous blocks

[44] On page 5 of the October 2019 report.

[45] Definition 6.29 of the ITU (2019).

[46] Definition 6.27 of the ITU (2019).

[47] See also the ITU's (2019) definition of hash function: "a function that maps a bit string of arbitrary length to a fixed-length bit string. Approved hash functions satisfy the following properties: 1. One-way: It is computationally infeasible to find any input that maps to any pre-specified output, and 2. Collision resistant: It is computationally infeasible to find any two distinct inputs that map to the same output". Definition 6.26 of the ITU (2019).

[48] The term "transaction" in DLT terminology is key and has a specific definition. According to Definition 6.61 of the ITU (2019) it refers to the "whole of the exchange of information between nodes. A transaction is uniquely identified by a transaction identifier". Arguably, the concept of exchange of information here refers primarily to an exchange of bits, however, behind the bits there is the content of the information exchanged between authorities.

in the chain, including the documentation submitted, may be made readable to selected participants (see Section 6).

5.4. Transparency

Another benefit would be a significantly improved level of transparency. If the blockchain solution chosen consists in integrating into the application all processes and decisions related to recognition, the amount of information available is vast. The receiving authority has a keen interest in information from other countries that could be uploaded and shared in the system. A key piece of information is when the authority of the country of origin withdraws the qualification of a particular individual. There is also an interest to be informed about changes in the training curricula in the country of origin: e.g. the authority could rely on the assumption that as long a no modification of a particular training degree is found in the system, it can safely continue to grant recognition to that degree without further verification of the curriculum.

If the system is open to more than two jurisdictions then the authority could access to even more information. First, in case it receives an application in respect of a degree that is not yet known to it, the authority could check in the system if other third country jurisdictions have recognised that degree recently, and if so chose to rely on that and avoid time-consuming verifications of the curriculum. In doing that it could see under what condition the recognition was granted (straight, or with additional requirements or tests). Second, the authority could be informed if and when the recognition of a particular foreign degree is revoked by others. If several revocations are notified by other authorities, the authority could check the situation.

The last two types of information are also interesting to the country of origin. A country of origin has an interest to know if the holders of its credentials use to seek recognition abroad and under what condition recognition was granted. It has an even keener interest to be informed about revocations of recognition of its credentials.

What about rejections of applications? Authorities would benefit from knowing if the applications for recognition of a given degree are denied by other third countries. However, that sort of information may be sensitive and it would be advisable to think twice. A system in which a reputational risk is at stake may be self-defeating. If it becomes widely known that the degree of a particular academic institution cannot obtain recognition, the reputation of the institution would suffer, and maybe the reputation of the country. “Performance”, in particular negative performance, in terms of recognition shall by no means become a substitute or a component for rankings. Rankings are already there to assess and make publicly known the quality of educational programmes. It is not the purpose of recognition procedures to interfere with that.

Another reason for being cautious with making rejections public is that an authority may reject an application for reasons that have no relation to the level of the qualification. For example, an authority may decide not to pursue an application because the applicant doesn’t meet the conditions required to obtain a work permit anyway. Such denial by abortion is sensible and makes sense to avoid that the applicant, the authorities of the country of origin and the receiving country waste their time and resources for no practical purpose. However, if others read in a ledger that a diploma from a particular institution was rejected they may draw the wrong conclusions.

Whatever the necessary restrictions to be implemented, it is rather obvious that the immediate availability of information pertaining to the work flow of receiving authorities and authorities of origin is the major benefit of blockchain, beside trust.

5.5. Traceability

Traceability has a prominent importance both in blockchain as a technology and in recognition as an administrative task. A recognition decision is not a single-shot administrative action. It has its own life. For example, if a recognition-holder commits professional faults or is found to be incompetent, the authority may want to understand exactly if, how and where in the recognition procedure a mistake may have been committed. If an application is submitted, the authority would check if it has already dealt with that applicant, including if it has already rejected an application from, or withdrawn a recognition to, that applicant and for what reason. Maybe the reason still prevails, or maybe no longer. It would be wrong to reject an application only because it appears in the system that a similar application was rejected in the past, without bothering about the reason. Similarly, if the reason still prevails, the authority would save time and resource if it can see the whole applicant’s history with a few clicks. Good traceability is good efficiency, and efficiency is among the goals of deploying e-administration.

A particular situation prevails in federal and decentralised jurisdictions. In Switzerland, a federal state, state recognition is a competence of the central authority. However, if a federal system provides that the recognition of a particular qualification falls into the sub-federal competence it is useful for sub-federal authorities to check for previous rejections or withdrawals in other constituent parts of the country. In short, it is very valuable in the administration of recognition if information never gets lost and cannot be tampered with.

Blockchain technologies represent a robust tool for traceability and auditing of administrative procedures because once uploaded the documents are frozen in time and can (almost) never be tampered with (see Section 5.2).

5.6. Efficiency

Another possible benefit might be a streamlining of the processes of the authorities involved. Some authorities work with efficient administrative tools and systems and have well-functioning archiving and tracking systems. However, that may not be the case for all. Joining a blockchain or some other ICT-based application might be the opportunity to review, modernise, streamline and transform administrative processes.

5.7. Smart contracts

One feature of DLT that is not expected to be retained by recognition authorities is automatic execution at any stage of the process. In the universe of recognition, there is no appetite for such thing like a “smart contract”, and all steps in the procedure would remain human-controlled. In that sense for the purpose of this article the main benefits of the technology would be confined to trust, efficient information exchange (transaction), transparency and traceability.[49]

6. Possible configurations of platforms for international recognition by states

6.1. Overall approach and architecture

Blockchain technology is flexible and programmable, and makes it possible to customise the configuration of an application to almost any needs of the users, and to attribute (and modify) users’ permissions.[50] Hybridation is always possible, such as hybrid permission systems,[51] or public/private hybridation. A smaller private blockchain may be

[49] A smart contract is not a contract in the legal sense but a self-executing code (programme) that automatically performs an action when pre-defined conditions are all met.

[50] The ITU (2019) defines “permission” as the “intended allowable user action (e.g., participate, read, write, execute)”, definition 6.41, p. 4.

[51] The ITU (2019) defines “hybrid permission” as “a combination of permissionless and permissioned accessibility”, definition 6.28, p. 3.

attached to a larger public one.[52] And a participant may always be allowed to choose with whom and when a particular information is being shared. Beck, Müller-Bloch and King (2018) summarised the typology of blockchains in the following table:

Access to Transactions	Access to Transaction Validation	
	Permissioned	Permissionless
Public	All nodes can read and submit transactions. Only authorised nodes can validate transactions.	All nodes can read, submit, and validate transactions.
Private	Only authorised nodes can read, submit, and validate transactions.	Not applicable

The configuration of a blockchain is closely linked with the number and nature of participants. If few participants want to administer procedures just among themselves, they would set up a small private blockchain. The question of participants is also linked with the question of who takes the initiative. In the private sector, one scenario could be that a programme developer simply establishes a blockchain platform, makes it available for participants to join, and receives fees (e.g. writing fees) in return. Such scenario is most unlikely for government applications and even more for intergovernmental ones. Two approaches are conceivable for governments. One is that a recognition authority takes the initiative alone, commissions and buys the programme, launches the platform and invites applicants as well as other authorities to open an account. The other approach is that a few national authorities conceptualise the initiative together and launch it jointly, and then invite applicants and other authorities to join. The question is whether other authorities would join the platform in spite of not having participated to its development. The most basic modality to join a system would be to download the programme, but this is cumbersome for the applicant. Thus it is important that the model specification requests more user-friendly interfaces.

Against this backdrop, two questions arise: interoperability and portability.

It is highly unlikely that an introduction of DLT would occur on the basis of one single universal platform. More likely than not, even if a transformative technological development in recognition procedures occurs, each participating country/authority or group of countries/authorities would operate from its own platform. This implies that a question to be addressed regarding such future development is how to ensure communication between platforms, respectively ensure that platforms are interoperable. Interoperability may be achieved at different levels.

Based on the more conservative assumption that the different blockchains would be built on different technologies/protocols, there would be a need for interoperability between the ledgers. The ITU defines inter ledger interoperability as the "ability of two or more distributed ledger protocols to exchange information and to use information that has been exchanged with one another".[53,54]

When it comes to government participation the question of joining an existing platform is not as straightforward as, say, for an individual wishing to start bitcoining. At the very least, the government should examine the question of data portability beforehand, because once a government has started to run some administrative procedures in a blockchain account its past data (the history of its past actions in relevant procedures) is somehow locked in there, and if the government later wants to move to another system (e.g., create its own platform) it would face that hurdle. This hurdle exists whether the blockchain is truly decentralised (which would not be the case for such a type of application) or is the initiative of one central actor. This will be discussed in Section 7.

In any case, the launching of a DLT-enabled recognition project implies that the authority or group of authorities taking the initiative mandates a programme developer to create a customised blockchain for that purpose, given that no such turn-key, ready to buy programmes exist on the market. Developing an e-recognition procedure with an available open source blockchain-based digital ledger software such as Hyperledger Indy[55] (see Section 7.3) is an appropriate approach.

6.2. Configuration of an e-recognition platform, step by step

In line with this whole article, this Section deals with official recognition of foreign diplomas by state authorities. Thus, it is not related to other situations, for example private schemes to ease verification of credentials between educational institutions and potential employers.

As said earlier, blockchain technologies are flexible and allow its users to define what they want to share, with whom, when and how. Recognition procedures feature a number of typical steps and types of action, and for each action a DLT-enabled solution may provide a number of technical options. The purpose of this Section is to consider step by step such typical actions and corresponding technical options in a kind of "fictive" example.

In the fictive system below, there are four classes of "must-have" blockchain participants located in at least two partner countries:

1. the applicants (individual persons),
2. the granting authority, i.e. the authority of the receiving country that is competent to grant recognition,
3. the authority of origin, i.e. the authority of the country of origin that is requested by a granting authority to validate the diploma, or the curriculum, or other information as the case may be,
4. other authorities involved in information verification or decision making, whether from the receiving country or the country of origin.

Those participants are a subset of the stakeholders listed in Section 5.1. The needs of the other stakeholders listed in Section 5.1 are addressed in Section 6.2.15, but those stakeholders are not indispensable participants for the proper administration of the recognition process.

As stated in Section 1.4 it is not the ambition of this article to propose a magic recipe. Accordingly, this Section only presents steps in the process and related technical options. The launchers of a DLT-based recognition procedure should examine such types of actions and options in depth in the development phase, identify the best solutions, or as the case may be decide to abandon the project or revisit the idea at a later stage.

Steps and actions are described in the headings, followed by considerations on possible technical implementation. The sequence of the headings more or less corresponds to the chronology of the work flow of a typical recognition procedure.

[52] The ITU (2019) defines "public distributed ledger system" as a "distributed ledger system which is accessible to the public for use", definition 6.49, and "private distributed ledger system" as a "distributed ledger system which is accessible for use only to a limited group of DLT users", definition 6.50, p. 5. This distinction is different from the concept of permission defined above. Whether in a public or private DLT system the participants may be required or not required permission to participate to, read, write, or execute specific actions or activities in the system.

[53] Definition 6.31 of the ITU (2019), p. 3.

[54] See also WTO (2018), p. 38.

[55] See <https://www.hyperledger.org/projects/hyperledger-indy> accessed 29 November 2019.

6.2.1. Opening an application procedure by an applicant

Two approaches to this could be proposed. If the blockchain is strictly private then the applicant should first contact the granting authority offchain,[56] for example through the authority's existing website. The granting authority would then accept the applicant's account in the blockchain. If, however the system developer deems that there is no reason to be so restrictive it could make the access unrestricted, allowing anyone to enter the blockchain and submit an application. In both cases the authority would require some type of proof of identity. A motive for the first approach may be because it permits to obviate access until such proof is received. As said in Section 6.1, both the private and the public blockchain may be either permissioned or permissionless. DLT systems (consortiums) may also not use blockchain.

A slightly distinct question is that of ascertaining that the person who opens the account and submits the application file is really the holder of the degree at hand (see Section 7.3).

More likely than not, there would be no need at this stage of the procedure to share this with other blockchain participants (other authorities).

A more liberal and desirable approach is that applicants submit all at once the application including the ID and proofs of qualification. In that case this and the following step would merge.

6.2.2. Submission of application by an applicant

Several ways may be offered to applicants for the submission of their files. As this issue is critical it should be thoroughly examined in the development phase of the project, in particular with all interested stakeholders (see Section 5.1). A basic idea would be that all documents are uploaded in the blockchain, however this would raise diverse serious issues, as explained *passim* in this article. An alternative to this would be to store only the hash of each document (e.g. hash of a degree, license, a certificate of work as proof of experience, etc.) in the blockchain and to have a parallel databank to upload the actual documents, allowing the authority to immediately check the documents and their conformity with the related hashes. In the long term, this would mean that the applicant may chose at any point in time to erase the actual documents and information. In terms of traceability it implies that only the hashes remain. Another alternative would be to upload only the hashes, being understood that the applicant keeps the documents available to the authority upon request. The two alternatives should not be seen as totally undermining the benefits of the application. True, if say after the denial of an application the applicant erases all documents and personal data, leaving only the corresponding hashes in the blocks, and years later applies again for the recognition of the same diploma, the authority would not find the said material unless it saved copies of them in a parallel databank. However, if when hashing the re-submitted diploma exactly the same hash is produced as the initial one, the authority would realise that this is a renewed application. In such case the authority would trace back the entire process of the first application.

Section 5.2 illustrated another use of hashes which is to allow the granting authority to compare the hash it has with the hash provided by the authority of origin. Two identical hashes imply that the diploma submitted by the applicant is authentic and not modified in any way. Obviously, this can't work for documents that exist only in one original. Typically, requirements of prior experience are verified on the basis of certificates of work, but a certificate of work is possessed only by the applicant, no one else. In that case there is no alternative to providing the actual copy of the document.

For the sake of completeness, as far as university diplomas are concerned, in case a system of digital diplomas or CeDiplomas exists in the country of origin, then a simple hyperlink between the two systems would suffice.

6.2.3. The granting authority requests additional information or documents from the applicant

Blockchain technology allows a participant to ask information from a particular other participant. Thus, technically speaking the request for additional information could be done onchain. However, the authority may prefer to make it offchain, e.g. by e-mail.

6.2.4. The applicant submits additional information or documents to the granting authority

This has to be done in exactly the same manner as the initial submission (see Section 6.2.2).

6.2.5. The granting authority requests information or validation from the authority of origin

Without prejudice to having direct contact by e-mail or phone, for the purpose of keeping a track record of the whole process the granting authority may prefer to convey such request through the blockchain. In case the authority places its request onchain, it would certainly not wish this to be shared with other participants.

6.2.6. The authority of origin provides information or validation to the granting authority

Crucially, this should occur in the blockchain for the e-application tool to deploy its full benefits. It is doubtful though that the granting authority and the authority of origin would be ready to grant reading rights to the applicant or to other authorities.

In respect of information of general nature this functionality of the project may well be criticised for being soon obsolete considering that governments should better ensure that relevant information on their education system (curricula, learning objectives, methods of assessments, etc.) are made publicly available on a dedicated website, as recommended by the UNESCO Global Convention (see Section 4.2). However, given the breath of the scope of professional recognition (which includes vocational training, experience gained, etc.) there will always be a need for direct requests for information and validation. Secondly, the fact of the matter is that it will take very long until even a meaningful number of countries are somewhere near providing complete information on their websites.

6.2.7. The granting authority grants recognition

If this step of the procedure is performed in the blockchain the recognition decision can (almost) not be tampered with, it can be seen by other participants allowed to read it, and it remains recorded "forever". In case only the hash of the decision is loaded, participants that receive the copy of the decision from the degree-holder could easily check if the hash of the copy of the decision is identical to the stored one.

The political will of authorities in respect of sharing that information on a broad basis is, indeed, the factor that would reinforce the case for using a blockchain technology. If the authorities are cautious and limit the access (reading rights) to the applicant only, or to the applicant and the authority of origin, then there is no much difference with today's situation. If there is political will to share with all others – consistent with applicable law including in respect of prior consent of the data owner – then there would be a quantum leap in recognition practice and the interest to adhere to the system may increase. As said in Section 4.2, knowing which degrees have been recognised in which countries, when and under what condition is a highly interesting information both for authorities around the world and for degree-holders contemplating recognition. For example, the recognition of a particular degree may be granted on the condition that some additional requirements are met. In some cases, a recognition is valid only for a limited duration of time. And recognition decisions that are limited

[56] "Offchain" means "related to a blockchain system, but located, performed or run outside that blockchain system", see definition 6.37 of the ITU (2019), p. 4.

in time may follow more lenient conditions. Such details are valuable information for participants.

6.2.8. The granting authority rejects recognition

As said in Section 5.4 this is a highly sensitive issue. More probably than not, this would be shared only between the applicant and the granting authority.

6.2.9. After recognition, a granting authority receives a tip of suspicion of fraud.

This would most probably occur offchain.

6.2.10. The granting authority checks the suspicion of fraud

As above.

6.2.11. The granting authority revokes recognition

It may sometimes happen that the authority revokes the recognition previously granted to a particular person. Though this is a delicate matter, it must be said that this type of information is most valuable to third parties. The EU IMI scheme (see Section 4.1) precisely aims at alerting participants in cases of fraud, in particular counterfeited credentials. In the IMI alert system, the full name of fraudsters is shared with all participating authorities. This approach is highly commendable. In case a recognition is revoked because the authority discovers *ex post* that a fraud was committed in the recognition process, or that the recognition-holder is otherwise not fulfilling applicable professional requirements, other authorities should be allowed to know that immediately, including the personal details of the person involved (subject to possible privacy rules on exchange of information between official authorities).

In blockchain systems of recognition privacy concerns may be addressed as the technology is flexible enough to maintain encryption on any particular piece of personal data that needs to be protected. For the scheme to deploy its full benefits, a balance must be found in which as a minimum any participating authority may know immediately whenever the recognition of a particular degree is revoked and preferably also the identity of the person (if consistent with the law).

6.2.12. The authority of origin withdraws the degree of a particular person

This type of situation (to be distinguished from the above one) may occur from time to time, and again it would be preferable to allow the technology to deploy its full benefit. Technical solutions should be implemented to allow any authorities that granted recognition to that particular person to be immediately informed of such withdrawal, so that they cancel the recognition granted.

6.2.13. The training curriculum or conditions for a degree are modified in a participating country

As explained in Section 4.2, authorities use to recognise foreign degrees without double-checking the content of the degree if they recognised that degree in the recent past, unless the submission by the applicant is clear enough for the authority to realise that there has been a recent change in the curriculum. That is why it would be valuable that authorities are expected to record in the blockchain any changes in curricula, admission requirements, assessment methods, or levels of their degrees even if they keep the same denomination. Nothing hinders sharing this with all participants in the scheme. As said in Section 4.2, an alternative is to provide the information on Internet websites.

6.2.14. Domestic interagency information sharing

Applicants seek recognition for a concrete purpose: exercising their professional activity in the granting country, whether on a transborder basis (without actually travelling to that country) or in the vast majority of cases on-site either as a non-resident supplier (short term stay) or by seeking employment and integrating the labour market. All those scenarios may apply either in the context of a relationship or contract between the company and a client, or within the same company or conglomerate (e.g. if part of the company's staff is posted abroad). When the practice of a professional activity involves the admission of the degree-holder in the granting country, the applicants would need entry permits and/or work permits from authorities other than the recognition authority. In some countries, the foreign degree-holder has to submit all relevant information to each authority approached, e.g. submit the recognition decision to the migration authority. In other countries some degree of interagency coordination is in place, either through conventional channels or with ICT solutions, under which the authorities would directly exchange the information relevant to the respective procedures they are competent for. That function could be integrated in the blockchain platform, allowing, say, the migration authority to directly check if a particular application for recognition has been submitted, is being processed or has be concluded. This would allow the authorities and the applicant to save time and resources.

6.2.15. Information of other stakeholders

As alluded to in Section 5.1 and 5.4 a number of other stakeholders may have an interest to access to some information. While technically speaking a broad array of possible configurations and parameters are conceivable, the choices would probably be made on the basis of 1) the applicable regulatory framework concerning the protection of personal data, and 2) the political will of the authority to share its data with other authorities and with the broader public. At the present time it seems that especially in terms of political will the practice is conservative.

The question could boil down to the level of disaggregation of information made available. The case of employers may serve as an illustration. Assume that a regulation prescribes that architects need a specific qualification to be authorised to work independently and sign architectural designs. As a result, applications for recognition will be submitted by independent foreign architects, and some foreign qualifications will be recognised for that purpose by the authority. Assume now that a company seeks to hire an architect as part of its staff. For mere employees no qualification requirements apply, and hence no recognition is needed. However, if foreign architects apply for an open position, the hiring company has a keen interest to know if the diploma of the applicant was ever recognised by the authority. If yes, the company would feel comforted that the diploma is robust enough. A similar interest prevails in respect of placement agencies, head hunters, and similar service providers.

Another case relates to recognition authorities of third countries. Assume country A, say Colombia, receives an application for recognition of a Swiss degree that it never handled in the past. That authority would be interested to quickly see if the authority of its neighbouring country B, say Peru, recently did recognise that degree. Again, if yes, and if Colombian and Peruvian requirements for the exercise of the profession concerned are the same, then Colombia may choose to rely on the precedent set by the Peruvian authority and process the application on the basis of the file provided by the applicant without double checking the exact curriculum with the Swiss authority.

Those two illustrative examples show that the need for information may well be met by allowing access to relatively aggregated data. Participants such as employers or third country authorities would of course love to access to each and every detail, but partial and aggregated information suffice to meet most of their needs. A listing of recognised degrees extracted from the system at regular intervals could also be good enough, as well as the possibility to search the system in respect of names of degrees and schools but not names of degree-holders. If needed, such function may be incorporated in the blockchain solution.

It may be posited that the authority of a third country that receives an application from a particular person is interested to know if that

person is already recognised in any other countries participating in the blockchain. Though the technology can support that, it must be underscored that providing a general right to read individual information in the blockchain raises privacy issues. In any case, the applicant is free to directly provide that information in his application to that third country. The sensitive issue of being informed of earlier rejections was elaborated earlier in this paper and needs not to be address again here.

7. Implementation challenges

After looking at the opportunities in Sections 5 and 6, it is equally important to understand the challenges. The thoughts offered in this Section are, again, strictly limited to the issue at hand as framed in Section 1.

7.1. Interoperability/standardisation

Given that in the case of recognition procedures of foreign qualifications the scheme chosen would unavoidably rely on inter ledger interoperability (see Section 6.1), the most obvious challenges pertain to interoperability. Interoperability (or standardisation) is often regarded as covering at least three levels: regulatory interoperability, semantic interoperability, and technical interoperability.[57]

Technical interoperability or standardisation is the lesser challenge as it would come with time. Reference may be made to the work of ISO Technical Committee ISO/TC 307 on standardisation of "blockchain and distributed ledger technologies".[58] Already now it is feasible to build large multistakeholder international blockchain systems with no interface problem, as the example of *TradeLens* proves (see Section 1). The question is thus not primarily whether technology is available, but whether those who launch a new platform ensure that it is interoperable with any already existing DLT platforms. However advanced the feasibility of technical inter ledger interoperability sounds, it doesn't represent the whole issue as it leaves aside the thorniest problem of interoperability with systems that are not ledger (or DLT) based. This latter class of interoperability is particularly relevant to data portability and legacy databases, which are dealt with below.

As to semantic interoperability, using a common language among authorities will be a challenge. Uncertainty about the meaning of terms used in diplomas and curricula is a major motive for a granting authority to seek clarification from the country of origin. The first hurdle is that there is no organisation competent to take up a role of standard-setter at the international level for all aspects of recognition (i.e. not just, say, within the Bologna Process). There would be the UNESCO Global Convention, but that treaty is limited to higher education and its obligations do not amount to a binding standardisation, as may be seen from the few quotes reproduced *passim* in this article. The UNESCO has also developed its International Standard Classification of Education (ISCED),[59] but it mainly serves statistical purposes and focusses on duration of curricula rather than actual content. Nevertheless, practitioners of state recognition in competent authorities routinely use ISCED to assess and compare educational levels of diplomas on a common basis.

Regulatory interoperability at the international level is not on the agenda. However, unlike the former two, regulatory interoperability is not an absolute must, because the approach, practice and degree of restrictiveness to recognition, as well as the qualification level required to exercise a profession may continue to vary from country to country without impinging on the feasibility of recognition procedures that would be more integrated than the current conventional ones. In other words, a country may be very liberal in terms of recognition policies and practices, and another country very restrictive, but each one would recognise the other's degrees according to its practice and that does not impinge on their ability to use the same blockchain platform. The needs here are not the same as, say, in terms of financial/prudential recognition. Yet, it is important to be aware of the common regulatory discrepancies of more formal nature. Each country has its own rules and regulations determining what documents may be accepted in electronic format (electronic copies), under which conditions and with which effect. These may differ from country to country. Regulations and procedures regarding authentication and requirements to translate documents may also differ, as well as accreditation practices.

In the present systems that are based on conventional tools (e.g. paper-based) those discrepancies are just accommodated by the current recognition practice. However, for a blockchain-based system to function smoothly and efficiently it is preferable not to overload the system with a host of particular procedures and transactional information about who uses to do what and how. An international standardisation of the aforementioned rules is unfortunately not on the agenda.

7.2. Protection of personal data and GDPR conformity

The vast majority of jurisdictions have a legal framework for the protection of personal data. Many non-EU countries aim to align themselves with the EU General Data Protection Regulation[60] (GDPR) with a view to meet their citizens' demand. Another more specific reason for GDPR alignment by non-EU countries is to obtain a recognition of the adequacy of their privacy legislation by the EU Commission,[61] or to meet the conditions of so-called GDPR *ad hoc* safeguards.[62] The Convention 108 on the protection of individuals with regard to the processing of personal data contains privacy principles very similar to the GDPR's, and non-European countries may adhere to it for the same reasons as outlined above (see for example (Bygrave, 2020), (Mantelero, 2020) and Pauletto, 2020b). The fact that blockchain needs to be assessed in respect of its conformity with the GDPR and other privacy rules was identified relatively early, in particular by Berberich and Steiner (2016).

The protection of personal data is an issue; however, it would be wrong to consider it as a critical one because in the case of a typical recognition process only few personal data are filed. In the Swiss practice the personal information that the authority requires is limited to what is necessary to process the application and deliver the recognition, which is the applicant's name, date of birth and address, and the only personal documents needed are the ID and diploma or other proof of qualification. At the end of the procedure, the decision of

[57] Other classifications exist, but are less relevant for the issue of official recognition. For example, Shi et al (2020) propose to classify the three level as: syntactic interoperability, semantic interoperability, and cross-domain interoperability.

[58] See <https://www.iso.org/committee/6266604.html>, especially the work programme available at <https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0> accessed 14 November 2019.

[59] Downloadable at <http://uis.unesco.org/en/topic/international-standard-classification-education-isced> accessed 14 November 2019.

[60] Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), published in O.J. L119/1.

[61] The EU legal provision on adequacy is found in Paragraph 1 of Article 45: "A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation". This in turn is based on Article 44 GDPR: "Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined".

[62] GDPR ad hoc safeguards are the Standard contractual clauses (SCCs) set out under Article 46 and the Binding corporate rules (BCRs) set out in Article 47.

recognition will also be part of the file. How far some or all of those fall within the scope to the applicable data protection legislation will depend from the jurisdiction. In case some authorities enquire more personal information than in the Swiss example above this may generate more headache and costs in terms of privacy and information security management. As said, the most sensitive piece of information is the withdrawal of a recognition decision.

When it comes to a suspicion of fraud in a process the situation may become critical, but such situations are not frequent (see Section 4.1).

Before deploying a DLT system it is thus indispensable to check its conformity with applicable data protection rules. Data protection rules differ too much across countries to make a detailed assessment here, however a general consideration of some parameters is appropriate. As regards the topic of this article, the main parameters to be checked and ensured relate but are not limited to the following rules.

Principle of freedom of prior consent: the user must be free to choose to have, or not have, personal data stored in the system. As discussed earlier in this article, this is technically possible however the development phase of the platform should ensure that parameters are set to fulfil that principle, e.g. to allow the user to upload hashes rather than actual personal data and keep personal data available elsewhere, i.e. offchain, to allow a verification of the hash (see Section 5.2 *in fine*).

Splitting data storage onchain and offchain could raise security issues as, if weakly protected, offchain data could be hacked and it is not possible to know who accessed or who has access to the personal data. However, in their study of blockchain application in the health sector Shi et al. (2020) note some advantages of offchain storage including the impossibility to access detailed medical record, and the fact that "it helps to reduce the throughput requirement significantly, since only transaction record and a few metadata are stored in the blockchain. Besides, data pointers stored in the block can be linked to the location of raw data in the off-chain database for data integrity".

Freedom to withdraw consent: given that the main aim of DLT systems is to make stored data impossible to alter or delete, there is *prima facie* a contradiction with the user's freedom to withdraw consent. Here again, the appropriate configuration parameters may technically be programmed in the system, but this should occur in the development phase, e.g. to allow the user to upload hashes rather than underlying personal data and loading personal data at a different level, where it may later be deleted. GDPR-compliant protocols can also be built in a way that allows data deletion in offchain locations. This would allow any individuals exercising their right to delete their personal data and request a service provider to delete the hash pointing to their personal offchain data.

Of course, the above considerations critically depend on the assumption that a hash is not regarded, under the applicable rules at hand, as data pertaining to an "identified" or "identifiable" person (using GDPR terminology), which in turn is correlated with the robustness of hashes against hacking, cracking and decryption, including at the age of quantum computing. The French CNIL (2018) concluded in its report that "[a]nother example is the deletion of the keyed hash function's secret key, which would have similar effects. Proving or verifying which information has been hashed would no longer be possible. In practice, the hash would no longer pose a confidentiality risk. Once again, the information would also need to be deleted in other systems where it has been stored for processing".[63]

Another principle of data protection is the right to rectification. It is worthwhile clarifying that in spite of the proclaimed immutability of data, rectification should not pose major problems in a blockchain. For example, in consensus with the other participants involved in the transaction (exchange of information), the data-owner may upload the needed correction in line with the "append-only" structure of the blockchain. Arguably, the wrong data remains (forever) in the block. If the rectification consists in erasing entirely a wrong entry or a no longer valid information, in line with the append-only structure it would mean that both the original dataset and its invalidation are stored next to each other. Another possibility is to host personal data in the blockchain and encrypt this data with a key or hash to access to the personal data in the blockchain. Upon request, the key linking to personal data can be deleted while keeping the personal data in the blockchain. This would allow to keep the data onchain but without any possibility to find it (data without key). In some cases, this could still be perceived as not good enough. This is what prompted the EU Blockchain Observatory and Forum (2018) to state that once personal data is recorded "it may be difficult to rectify or remove it. Defining what can be considered erasure in the context of blockchains is under discussion".[64] An example of a reason for embarrassment is if the degree-holder was married at the time of application and then divorces and moves out of the original home: the blockchain would keep the address of the ex-spouse, and next to it indicate the new address.

A frequent component of data protection legislation is the obligation for participants to ensure the technical integrity of their systems, especially against hacking. Besides the storage of data, their safe transmission is necessary to guarantee data protection. Taylor et al. (2020) stated in their thourough examination of blockchain applications in the realm of cybersecurity that "[u]ndoubtedly, there are worthy applications for blockchain, however, a decentralized, trustless system cannot by itself solve all problems one may uncover in the field of cyber security". A technical solution for that is, for example, the use of encrypted tunnelling channels between participants. Given that recognition is conducted by government agencies there is a cyber security issue, considering that state-on-state malicious cyber operations are frequent and will forseeably remain so (Pauletto, 2020a).

Other approaches to comply with GDPR are to use private or enterprises blockchains that restrain access to sensitive information to a limited number of entities (competent units in government administrations), hence reducing the probability of data breaches.

As a matter of fact, the decentralised storage typical of DLT provides several rather than one entry point for malicious actors to gain unauthorised access to data. To that extend it is not an optimal architecture in terms of protecting data from unauthorised access. Another approach would be to break the fundamentals of blockchain by hosting personal data in a centralised back end blockchain system.

In sum, blockchain technologies provide ways to address the challenge of privacy protection. DLT-based systems are difficult to crack; thus, data is at least as safe as in other Internet-enabled systems used by the authority. When uploading data on the platform the data-owner may chose with whom what data is shared and when.

When it comes to blockchain application in practice, the European Parliament (2019) is probably on the safe side in concluding that "the compatibility of these instruments with the [GDPR] can only ever be assessed on a case-by-case basis", and that "it is not possible to assess the compatibility between 'the blockchain' and EU data protection law", "it is impossible to state that blockchains are, as a whole, either completely compliant or incompliant with the GDPR". Thus, in essence, the European Parliament maintains the same conclusion as Millard (2018) in his broader study not limited to the GDPR, namely that "the appropriate answer to the question of whether a blockchain may be used to process personal data is not binary but rather 'it depends'. Undoubtedly, there remains a lot of work to be done".

Some standardisation work pertaining to privacy in the blockchain is in progress under the ISO Technical Committee 307.[65]

[63] On pages 8-9 of the report.

[64] On page 5 of the report.

[65] In particular ISO/TR 23244:2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations, available at <https://www.iso.org/standard/75061.html>.

7.3. Identification and the KYC-principle

In a host of potential blockchain projects the difficulty of ascertaining the real identity of the physical user of the computer connected to the platform was often a major challenge and is sometimes enough to shelve the contemplated project. In the practice of recognition, the situation is not so critical. In many cases, such as in Switzerland, in line with administrative efficiency the authority would accept a mere photocopy (for paper application) or a scan (for online application) of the identity document of the applicant. Who exactly is handling the procedure on the applicant's side is not considered as crucial, even more so because in practice the procedure is often administered by the company employing the degree-holder, or even by some external service provider. The author of this paper knows no instances where a certified copy of the ID is requested in the context of a recognition procedure. By analogy, in a DLT-based process (or any other e-government process) the applicant would have, at most, to upload a scan (respectively to upload the hash in the ledger and the actual scan on a conventional databank).

Still, in the unlikely case that an authority would wish to obtain certainty about its counterpart's identity blockchain solutions exist. For example, a basic way to handle that is that the applicant could be requested to ask the local authority competent for the civil registry or citizenship to validate the identity in the blockchain. The applicant could be requested to undertake a similar step with a consular office. This would increase the cost of the formality. But soon, as presented in the Section 1.3, more convenient solutions will exist: digital IDs and self-sovereign identities solutions will gain momentum. The EU Blockchain Observatory and Forum (2019) concluded that "it is now possible to build new identity frameworks based on the concept of decentralised identities – potentially including an interesting subset of decentralised identity known as self-sovereign identity (SSI)".

It is important to recall that eID and eSignature are performing two main functions, as laid out by (Lentner and Parycek, 2016). Those are the process of identification and of authentication. Identification "means the process necessary to perform unique verification or determination of identity" while authentication "means the genuineness of a declaration of intent or an act". DIDs are helpful when the applicant is the degree-holder, but of limited of no help when the application is administered by the company.

The structure of DID concepts may bring some drawbacks. Mohsin et al. (2019), recalling that "[u]sers are required to log in to a reliable authentication server with a user ID and password and afterwards to third parties with a trusted authentication system" conclude that "[t]he problem is that denial of service attacks and technical failure can lead to the inefficiency of the trusted third party. The design of an authentication scheme which is user-friendly and independent of a trusted party remains a challenge". And DoS attacks are a typical modus operandi as intensified cyber warfare operations among and against states may be witnessed (Pauletto, 2020a).

The open source blockchain-based digital ledger software Hyperledger Indy mentioned in Section 6.1 is an effective way to address the issue of digital identity in a blockchain recognition procedure. A recognition authority that launches a blockchain solution (or any other digital solution for recognition) could accept selected digital identities as proof of identity for that purpose. Some countries, such as Switzerland,[66] have their own country-specific digital ID projects, but since recognition is by definition intended for foreigners the national DID solution would not be the relevant one.

A comprehensive review of the e-ID literature and research is provided by (Melin et al., 2016). Some standardisation work pertaining to identity management in the blockchain is in progress under the ISO Technical Committee 307.[67]

7.4. Data portability

All technologies of data management raise issues of portability of some sort, but due to its structure it seems that DLT is a case in point. Broadly speaking, there are two classes of portability limitations. One is where an updated version of a system differs so much from its previous release that part of the content (say, some files) cannot be read or processed, or are subject to bugs. The other is when replacing one system with another. Uncertainties about the portability of data is what sometimes prompt companies or governments to delay transformative decisions. In the case examined in this article, one predictable path would be that an authority is solicited to participate, as a country of origin, into the recognition blockchain initiated by other authorities in receiving countries. In doing so, the solicited authority would have the track record of its activities stored there. Thus, the day the said authority decides to set up its own solution, hurdles may arise in migrating its files.

In some countries, the hurdle may not need to wait until the day an alternative e-recognition system is implemented. Sometimes, administrative files are moved from the operational units of a government into a centralised state archive after a number of years. What happens when part of the archive is in the blockchain platform launched by country X? How will the migration be organised?

If participating to a blockchain-based procedure means that all files need to be stored twice, onchain and in the conventional system in view of a future smooth migration, then the incentive to participate would be low.

7.5. Liability

Another issue relates to liability, whether in respect of the quality of the information supplied into the chain, or in respect of the way to use such information. Of course, blockchain is simply a technology and no more than that and thus it provides no assistance as to what occurs in the real world, *i.e.* offchain. However, in jurisdictions such as Switzerland liability is not regarded as an issue in recognition processes because as long as due diligence was followed in administering an application no liability may arise, even if, say, a falsified diploma was recognised, and later the recipient of the recognition causes injury to a client or patient. And in any case, before the liability of the recognising authority may be engaged an adequate causality with the injury incurred would need to be proven, which is a quasi-impossible endeavour.

7.6. Speed

It is known as a fact that DLT systems are slow. Very slow. This challenge is correlated with the number and nature of objectives or conditions required by a particular blockchain use case. This is especially true of requirements in terms of privacy (see above). As Peng et al. (2020) noted in their piece on privacy preservation in blockchain, "[t]he blockchain itself confronts severe efficiency problems like low throughput, while smart contract based on blockchain suffers from high computation overhead". Therefore, they add, the privacy schemes should be designed so as to avoid "efficiency degradation of the blockchain system". Examining specific privacy protection mechanisms Feng et al. (2019) state that "mixing methodologies incur an

[66] SwissID is a joint venture of state owned enterprises and private companies issuing a DID for Switzerland, <https://www.swissid.ch> accessed 3 December 2019.

[67] In particular ISO/DTR 23249 Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management, available at <https://www.iso.org/standard/80805.html>, and ISO/WD TR 23644 Blockchain and distributed ledger technologies - Overview of trust anchors for DLT-based identity management (TADIM) available at <https://www.iso.org/standard/81773.html>.

additional waiting delay. The complex cryptographic primitives […] normally bring about heavy computation and communication overhead".

However, in the case of recognition speed is not assumed to constitute a key expectation, at least on the applicant's side. Thus provided that it does not exceed a certain tolerance level, this inherent lack of speed has no major consequence on acceptance or user value.

7.7. Scalability

It is also known as a fact that DLT systems can be scaled up only to a given limit. The higher the transmission overheads (see Section 7.6) and the further limited the scalability. However, except in the unlikely scenario of a universal recognition platform encompassing all countries, the type of application hypothesised in this article is expected to be of a manageable size. Any such application – assuming it is rolled out one day – would probably involve few sponsoring recognition authorities plus some more authorities. The number of recognition decisions per year is reasonable compared to other government use cases because recognition concerns only foreigners, not nationals, and because a degree-holder normally applies only once in a lifetime for recognition in a particular country. More importantly, in case there is a predictable risk of overload it is possible to design and operate the system at two levels, the DLT-proper level where hashes are stored, and a conventional database level for storing documents.

7.8. Critical mass and fragmentation

An expected headache for implementing a blockchain technology in recognition procedures relates to the participation. There is first a challenge of critical mass. Two jurisdictions could deal with each other through their own joint blockchain, but then the added value compared to a conventional technology would be close to nil. A growing number of participants is thus a necessity, but even then, there will always be a large number of countries and authorities that will not join or not undertake to take up a blockchain technology. As a consequence, authorities will anyway have no choice but to run two parallel working methods, one based on a blockchain and one on conventional methods. Assuming that authorities of each country or country group would have their own platform and blockchain technology/protocols (see Section 6.1) the overall outcome may leave a sentiment of fragmentation. On the practical side, those considerations raise some questions given that "many public networks have a limited capacity to interface with other DLT protocols, legacy databases [inherited from the pre-blockchain era] and non DLT systems".[68] The scenario to avoid is ending up with a variety of parallel recognition blockchains that cannot communicate with one another. There are currently several projects tackling the challenge of cross-chain transactions (e.g. Polkadot, Cosmos Hub).[69] Also, the two-way peg and cross-chain atomic swaps are first steps in that direction. (See also Section 7.1).

7.9. Risk of overshooting

On a totally different score a final challenge is overshooting. Often, the introduction of a new technology that opens new frontiers induce developers to use it to the fullest possible extent. This might be counterproductive though. In particular, new technologies shall serve to simplify administrative processes, not encourage some authorities to multiply the controls and create an inflation of control items simply because they happen to have a tool to do it. All too often, digitation of conventional administrative procedures result in the implementation of a "control by design" solution even when in the conventional process those control items where not considered worth the effort. Doing so often defeats the initial purpose of the project: streamlining, facilitation and speed of transaction. The reason for ht eundue occurrence of "control by design" solutions is that unlike conventional systems, the development of digitised systems are too often approached more from a technology perspective rather than with a big picture of real purpose, service, user value and benefits.

All the above challenges may sound chilling. Maybe; if two dimensions are disregarded. First the fact that technology is improving fast and always faster. Second, the fact that e-government is more and more a benchmark in public administration. With time, the challenges will weigh less in the balance and the opportunities will weigh more. When e-government will become the norm, then recognition procedure will have to opt for a new approach as well. The soonest the reflexion starts, the better.

8. Conclusion

In an increasingly globalised world, the interest for projects of "transborder digitisation" or "cross-border digitisation" gains momentum. At the same time, recognition of foreign professional qualifications becomes increasingly relevant for individuals and for regulatory authorities, as people are increasingly moving across borders. Blockchain has never been considered in the realm of official recognition of foreign qualifications for authorising the exercise of regulated occupations, but there may be understandable reasons for this apparent lack of interest thus far. This may have to do with the caveat formulated by Gürkaynak, Yılmaz, Yeşilaltay, and Bengi (2018), namely that "talking about blockchain's future at this very early stage is almost like speculating about the future of the internet back in the 1980s". In the past year, however, besides the exponential progress in technology several changes occurred. Those developments make it necessary to provide a fresh insight into this issue.

First, academic recognition, the twin brother of professional recognition, has gained political profile in the international community with the conclusion of the UNESCO Global Convention, which also sets out several common principles on recognition. Second, a few countries have implemented systems of electronic diplomas, in addition to CeDiplomas already launched by individual universities. Third, systems of digital identities (DIDs) and self-sovereign identities (SSI) have emerged on the marketplace and are in use. And fourth, international work on blockchain in particular standardisation has advanced, mainly under the auspices of the ITU. Taken altogether these recent developments are paramount for the topic at hand.

This article contributes to research on two scores. First it confronts the functionalities of blockchain with the needs of recognition stakeholders, and concludes that they coincide nicely (Section 5). Second, and more importantly, it analyses all potential challenges or limitations of blockchain in view of the constraints imposed by recognition and proposes ways to solve or go around them (Section 7). Based on that, and on a concrete possible configuration of a blockchain recognition platform proposed in Section 6, this article concludes that while blockchain offers several opportunities and advantages, there remain some specific challenges that call for further technical developments before governments are expected to embark on such a project. Even though the bulk of the literature on blockchain and diploma-related issues seem to focus on the challenge of privacy, the author of this article rather opines that interoperability, portability and risk of fragmentation will need more time to be "solved" through technology developments compared to privacy concerns. The overall challenge that comes after all specific challenges are solved is to avoid that in order to meet all the constraints of recognition the blockchain solution offered is so much altered that the initial unique advantages of the technology are no longer exploited to

[68] Francisco Sarrias, presentation on Functioning solutions to DLT and non-DLT interoperability, made at the ITU Workshop on Distributed Ledger Technology Scalability and Interoperability, <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201908/Pages/programme.aspx> accessed 9 November 2019.

[69] See <https://polkadot.network/>, <https://github.com/cosmos>.

their fullest potential, rendering the technology as such not much more attractive than any other technology.

The main functionalities (and user values) that DLT solutions carry for the purpose of recognition procedures are: trust, information exchange (transaction), transparency and traceability (Section 5). Scholarly research on the problems faced by recognition authorities, in particular issues that relate to trust and fraud, is sparse and no quantitative information exist. Still, it can hardly be objected that a trust-related issue of some magnitude exists. In addition, it is a fact that the main role of recognition authorities consists in systematically checking the authenticity of documents and the actual content of training (curricula, examinations, experience gained at work, records of achievements, registration, etc.) in a large number of foreign countries. To make sure that authorisations to practice in a given jurisdiction are well monitored it is necessary to keep a good track record and traceability of all recognition decisions and the conditions under which they were reached. Information on recognition decisions is interesting to a number of stakeholder, which is why transparency would play an important role. Finally, recognition processes often require exchange of information (transaction) between authorities of the countries of destination and of origin.

In sum, all main functionalities of DLT solutions, the "four Ts", would be relevant in the case of an e-recognition procedure. This represents an opportunity for the adoption of blockchain.

Opportunities must always be confronted with limitations and challenges. This article identifies the following ones: interoperability, protection of personal data, user identification, portability, liability, speed, scalability, risk of overshooting, critical mass and fragmentation. The relevance of those challenges varies greatly, interoperability being probably the most serious one, and liability probably not that much.

This article attempts to point to solutions, existing or prospective, to mitigated them as technology develops and as e-government becomes a norm in public administrations. DLT has experienced remarkable improvements in the past few years and if it continues on that trajectory its disruptive potential on a wide range of private and public sectors is real. But to realise this potential, in particular in the case at hand, it is necessary that developers address the aforesaid challenges. To contribute to the work on future developments, this article offers some views on stakeholders and stakeholders' interests in the context of a possible e-government application for recognition of foreign qualifications.

A frequent mistake is to adopt a technology just for the sake of the technology. But in turn it is often too short to blame the technology after some projects failed. Whatever the technological environment, people will always remain at the centre, and the fact of the matter is that often projects fail because stakeholders' acceptance could not be mobilised, and this in turn is a result of lack of public value and poor stakeholders' management. Even in the case of recognition procedures of foreign professional qualifications, which is comparatively limited in scope, the community of potential stakeholders is stunningly broad. Hence a thorough analysis of stakeholders' interests is a prerequisite in any project of DLT-based recognition (Section 5.1).

Finally, another aspect to underscore is that in case new technologies are introduced, they shall serve good purposes, and not defeat the purpose of recognition or have undesired effects. In particular, new technologies shall serve to simplify and facilitate administrative processes, not encourage some authorities to multiply the controls and create an inflation of control items simply because it becomes possible. This is an example of what would turn many stakeholder groups against the innovation.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

I express my grateful thanks to the International University in Geneva (IUG) for funding this publication, to Frédéric Berthoud, head of the Recognition Division at the Swiss State Secretariat for Education, Research and Innovation, for his highly valued ideas and views on this project, to Virginia Cram-Martos, former Director of the Economic Cooperation and Trade Division at UNECE, for the stimulating discussion and suggestions during the WTO Blockchain Forum, as well as to Claudia Vanegas, executive assistant at the representation of Japan to ICAO, Blanca Anggela Zutta, officer in the Course Design and Training Section of the WTO, and the anonymous peer-reviewers for their much appreciated review of the manuscript. All remaining errors are my own.

References

Badr, A., Rafferty, L., Mahmoud, Q., Elgazzar, K., & Hung, P. (2019). A permissioned blockchain-based system for verification of academic records. In Proceedings of the 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). doi: 10.1109/NTMS.2019.8763831. <https://www.researchgate.net/publication/334484872_A_Permissioned_Blockchain-Based_System_for_Verification_of_Academic_Records>.

Beck, R., Müller-Bloch, C., & King, J. (2018). Governance in the blockchain economy: A framework and research agenda, Journal of the Association for Information Systems, 19(10):1020–1034, October 2018. <https://www.researchgate.net/publication/323689461_Governance_in_the_Blockchain_Economy_A_Framework_and_Research_Agenda>.

Berberich, M., & Steiner, M. (2016). Blockchain technology and the GDPR – How to reconcile privacy and distributed ledgers? European Data Protection Law Review, 2 (3):422–426. <https://edpl.lexxion.eu/article/EDPL/2016/3/21>.

Bonina, C. M., Cordella, A. (2009). Public sector reforms and the notion of "Public Value": Implications for eGovernment deployment. AMCIS 2009 Proceedings. 15. <https://aisel.aisnet.org/amcis2009/15/> accessed 14 November 2019.

Castelnovo, W. (2013). A stakeholder based approach to public value. Paper presented at the 13th European Conference on eGovernment (ECEG). Como, Italy. <https://www.researchgate.net/publication/259962817_A_stakeholder_based_approach_to_Public_Value> accessed 14 November 2019.

CNIL (Commission Nationale de l'Informatique et des Libertés). (2018). Blockchain: Solutions for a responsible use of the blockchain in the context of personal data, 6 November 2018. <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> accessed 20 October 2019.

Conte de Leon, D., Stalick, A. Q., Jillepalli, A. A., Haney, M. A., & Sheldon, F. T. (2017). Blockchain: Properties and misconceptions, Asia Pacific Journal of Innovation and Entrepreneurship (APJIE), 11(3):286-300. <https://www.emerald.com/insight/content/doi/10.1108/APJIE-12-2017-034/full/html>.

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges, Technology in Society, 62, in press. <https://www.sciencedirect.com/science/article/pii/S0160791X20303067>.

European Commission Joint Research Centre (2017). Blockchain in Education, by Alexander Grech and Anthony F. Camilleri, JRC Science for Policy Report, Seville, Spain, EUR 28778, doi: 10.2760/60649.

European Union Blockchain Observatory and Forum (2018). Blockchain and Digital Identity, thematic report published 2 May 2018. <file:///D:/Blockchain%20and%20recognition/EU%20Blockchain%20Observatory%20and%20Forum,%20Blockchainand%20Digital%20Identity.pdf> accessed 20 October 2019.

European Union Blockchain Observatory and Forum (2019). Blockchain and the GDPR, thematic report published 16 October 2019. <file:///D:/Blockchain%20and%20recognition/EU%20Blockchain%20Observatory%20and%20Forum,%20Blockchain%20and%20GDPR.pdf> accessed 20 October 2019.

European Parliament. (2018). Blockchain: a forward-looking trade policy, (2018/2085 (INI)) Committee on International Trade, A8-0407/2018, PE 625.465v02-00, 27.11.2018. <https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.pdf>.

European Parliament. (2019). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 634.445, July 2019. <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf>.

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system, Journal of Network and Computer Applications, Volume 126, 15 January 2019, pp. 45–58. <https://doi.org/10.1016/j.jnca.2018.10.020> accessed 14 November 2019.

Gürkaynak, G., Yılmaz, İ., Yeşilaltay, B., & Bengi, B. (2018). Intellectual property law and practice in the blockchain realm, Computer Law & Security Review: The International Journal of Technology Law and Practice, 34(4):847–862. <https://doi.org/10.1016/j.clsr.2018.05.027> accessed 14 November 2019.

Grolleau, G., Lakhal, T., Mzoughi, N. (2008). An introduction to the Economics of Fake Degrees, Journal of Economic Issues, 42(3):673–693. <https://www.tandfonline.com/doi/abs/10.1080/00213624.2008.11507173>.

Helliar, C. V., Crawford, L., Rocca, L., Teodori, C., & Veneziani, M. (2020). Permissionless and permissioned blockchain diffusion, International Journal of Information Management, 54, in press. <https://www.sciencedirect.com/science/article/abs/pii/S0268401219314586>.

ITU. (2019), ITU-T technical specification FG DLT D1.1 distributed ledger technology terms and definitions. ITU-T Focus Group on Application of Distributed Ledger Technology, 1 August 2019. <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf> accessed 24 October 2019.

Kopyto, M., Lechler, S., von der Gracht, H. A., & Hartmann, E. (2020). Potentials of blockchain technology in supply chain management. *Technological Forecasting & Social Change*, 161. in press. <https://www.sciencedirect.com/science/article/abs/pii/S0040162520311562>.

Lentner, G. M., & Parycek, P. (2016). Electronic identity (eID) and electronic signature (eSig) for eGovernment services – a comparative legal study. *Transforming Government: People, Process and Policy, 10*(1), 8–25. https://doi.org/10.1108/TG-11-2013-0047. accessed 14 November 2019.

Maringe, F., & Foskett, N. (2013). *Globalization and Internationalization in Higher Education: Theoretical, Strategic and Management Perspectives*. ISBN: 9781441132772.

Mavilia, R., & Pisani, R. (2019). Blockchain and catching-up in developing countries: The case of financial inclusion in Africa. *African Journal of Science, Technology, Innovation and Development*, 1–13. https://doi.org/10.1080/20421338.2019.1624009. <https://www.researchgate.net/publication/334949992_Blockchain_and_catching-up_in_developing_countries_The_case_of_financial_inclusion_in_Africa> accessed 14 November 2019.

Melin, U., Axelsson, K., & Söderström, F. (2016). Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective. *Transforming Government: People, Process and Policy, 10*(1), 72–98. https://doi.org/10.1108/TG-11-2013-0046. accessed 14 November 2019.

Millard, C. (2018). Blockchain and law: Incompatible codes?. *Computer Law & Security Review, 43*(4), 843–846. https://doi.org/10.1016/j.clsr.2018.06.006. accessed 14 November 2019.

Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Albahri, A. S., Alsalem, M. A., & Mohammed, K. I. (2019). Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. *Computer Standards & Interfaces, 64* (41–60). https://doi.org/10.1016/j.csi.2018.12.002. accessed 14 November 2019.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, Government Information Quarterly, 34(3):355-364. <https://www.sciencedirect.com/science/article/pii/S0740624X17303155> accessed 14 November 2019.

Panagiotopoulos, P., Klievink, B., & Cordella, A. (2019). Public value creation in digital government, Government Information Quarterly, 36(4), editorial. <https://www.sciencedirect.com/science/article/abs/pii/S0740624X19304101>.

Pauletto, C. (2020a). Information and telecommunications diplomacy in the context of international security at the United Nations. *Transforming Governments: People Practice and Policies, 14*(3), 351–380 https://www.emerald.com/insight/content/doi/10.1108/TG-01-2020-0007/full/html.

Pauletto, C. (2020b). Options towards a global standard for the protection of individuals with regard to the processing of personal data. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 58*. https://doi.org/10.1016/j.clsr.2020.105433. in press.

Peng, L., Feng, W., Yan, Z., Li, Y., Zhou, X., & Shimizu, S. (2020). Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks*. in press.

Poell, T., Nieborg, D., & van Dijck, J. (2019). Platformisation. *Internet Policy Review – Journal of Internet Regulation, 8*(4) https://policyreview.info/concepts/platformisation.

Rodrigues, B., Franco, M., Scheid, E. J., Stiller, B., & Kanhere, S. (2020). A Technology-driven overview on blockchain-based academic certificate handling. In Chapter 10 of R. Sharma, H. Yildirim, G. Meric (Eds.), Blockchain Technology Applications in Education, IGI Global, pp. 197-223, ISBN 978-1-522-59478-9.

Jennifer Rowley E-government stakeholders – Who are they and what do they want? International Journal of Information Management 31(1):53–62. <https://www.researchgate.net/publication/223896249_E-Government_stakeholders_-_Who_are_they_and_what_do_they_want> accessed 14 November 2019.

Scott, M., DeLone, W. H., & Golden, W. (2016). Measuring eGovernment success: a public value approach. European Journal of Information System. 25(3):187–208. <https://link.springer.com/article/10.1057%2Fejis.2015.11> accessed 14 November 2019.

Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security, 97*. in press.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks, 6*(2), 147–156. https://doi.org/10.1016/j.dcan.2019.01.005. accessed 20 May 2020.

Twizeyimana, J. D., & Andersson, A. (2019). The public value of E-Government – A literature review, Government Information Quarterly, 36:167–178 <https://www.researchgate.net/publication/331092224_The_public_value_of_E-Government_-_A_literature_review> 2019 accessed 14 November 2019.

World Trade Organization WTO (2018), Can Blockchain Revolutionize International Trade, by Emmanuelle Ganne, WTO publication.

Bygrave, L. A. (2020). *The "Strasbourg Effect" on data protection in light of the "Brussels Effect": Logic, mechanics and prospects*. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 38*. https://doi.org/10.1016/j.clsr.2020.105460. In press.

Mantelero, A. (2020). The future of data protection: Gold standard vs. global standard. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 38*. https://doi.org/10.1016/j.clsr.2020.105500. In press.

Warkentin, Merrill, & Orgeron, Craig (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management, 52*. https://doi.org/10.1016/j.ijinfomgt.2020.102090. In press.

Abbott, Kenneth W., Keohane, Robert O., Moravcsik, Andrew, Slaughter, Anne-Marie, & Snidal, Duncan (2000). The Concept of Legalization. *International Organization, 54* (3), 401–419. https://doi.org/10.1162/002081800551271.