Blockchain and smart contracts for education

Ramos-Sosa, Maria del Pino and Cabrera, Domingo and Moreno, Bernardo

Loyolabehlab. Universidad Loyola Andalucía, Universidad de Málaga, Universidad de Málaga

6 July 2020

Blockchain and Smart contracts for Education

María del Pino Ramos-Sosa,[1] Domingo Cabrera,[2] Bernardo Moreno[3]

Abstract

Currently, the preparations of the exams are made by the teaching or responsible teams to evaluate the students or applicants through an objective test to subsequently get a grade. We propose a system based on the use of Blockchain technology and smart contracts that would allow an automated preparation of test-type assessment tests, and the registration of the answers in a Blockchain ledger. The record of the answers made is registered chronologically, guaranteeing that the answers and the grades will not be modified, in addition to allowing the student to have access to that information (with prior consent). We also propose that the test's questions be obtained from a "question pool", previously filled in by experts in the field, and classified by level of difficulty, what would allow the assessors or students to establish the level of difficulty of the test. This would allow the creation of a more enriched curriculum for each student, *the student wallet*, a wallet containing the scores of exams, and the level in which students have accomplished the competencies and the skills acquired throughout their academic experience.

Keywords: Educational technology evaluation, Blockchain, Smart contracts, Competencies, Student wallet.

[1] *Loyolabehlab*, Universidad Loyola Andalucía. Avda. de las Universidades s/n. 41704 Dos Hermanas, Sevilla, Spain. Tel.: +34 955 641 600 (Ext. 2534). E-mail: mpramos@uloyola.es.
[2] PhD Program in Economics and Business, Universidad de Málaga, Málaga, Spain. E-mail: domingo.cabrera@uma.es.
[3] Departamento de Teoría e Historia Económica, Universidad de Málaga, Campus El Ejido, Málaga, Spain. E-mail: bernardo@uma.es.

1. Introduction

Quality of education is of great importance in today's era of knowledge and information, since today's society has the generation with the greatest access to education of all times. This has engendered the appearance of new institutions issuing certificates, with the consequent increase in the development and supply of new undergraduate and postgraduate degrees. Yet, in terms of quality of education, institutions keep providing to employers just the information regarding students' degree and transcripts, leaving aside the degree to which skills and competencies have been assimilated by students during their academic period. Indeed, the prestige of the institution issuing the certificate keeps being one of the key signals that clearly affects students' future in the labor market.

With the increase in the number of degrees and institutions available, there is also a greater risk of fraud. For instance, during 2018, several Spanish politicians were accused of earning a master's degree without attending classes or defending their dissertation (Stephen Burgen, 2018). This is a controversial issue that can have a negative impact on the prestige of the institutions (e.g., universities), and on the professionals involved in it (e.g., teachers and administrative staff). More importantly, students are the most damaged. They invest time and money in acquiring certain skills required to obtain employment, and they are seriously affected by any fraud or negligence carried out by institutions, teachers, other students' or third parties' actions of any kind.

The existing education system has considerable weaknesses that could call into question its prestige and reputation. As to institutions, the current system, as it is implemented, cannot ensure at a 100% level that a degree certificate or the transcripts are unfalsifiable, with the institution itself potentially being involved in a case of fraud.

As for teachers, it is expected that they apply their high degree of responsibility and professionalism in adapting their teaching activities to provide quality educational content in class. It is taken for granted that they carry out their teaching activities based on the content included in the syllabus of the subject; the material taught in class; the evaluation system; and the correction of the different assigned evaluation tasks. However, there may be teachers who commit malpractice by favoring or harming certain students for various reasons: the total content of the subject is not evaluated or taught appropriately, or the grade assigned to the student does not reflect his or her true performance.

Finally, the current system does not guarantee students are acquiring the maximum benefit from their educational experience. First, it is not verified whether the complete content of the subject is taught, which imply situations in which high-level learning objectives are not reached. Second, students must wait considerable time until scores are published. After that, they have the possibility to revise their exams and, under this situation, there is always some uncertainty whether the exam correction criteria applied in his or her case is similar to the one applied to the rest of the students. In fact, the door is open to find students receiving favorable treatment, being them able to bribe both teachers and administrative staff.

To deal with these and other weaknesses, we propose the introduction of Blockchain technology and Distributed Ledger Technology[4] in the education system. Merriam-Webster defines Blockchain as "a digital database containing information that can be simultaneously used and shared within a decentralized, publicly accessible network" (*Merriam-Webster*, 2020). It is a peer-to-peer system of information

[4] Although both terms are not equivalent, we refer to them collectively unless otherwise specified. The main difference is that Blockchain technology stores information creating chains of blocks and the distributed ledger does not. This is also conditioned on whether the ledger is permissioned (permission is needed to have access to the ledger) or permisssionless (Rutland, 2017).

transaction in which the information is recorded in chronological order and grouped in blocks, in a ledger which is distributed among the parts belonging to that network. Such system is totally decentralized, i.e., it does not need the support of any intermediary to certify the content of the information.

We propose a simple model in which we use Blockchain technology and Smart contracts to prepare, conduct and evaluate exams. Besides, once exams are evaluated the information regarding scores and skills acquired by the student will be issued by the institution and will be saved in a wallet for each student that we call "the student wallet". With this set of platforms, we try to minimize the weaknesses of the education system that we mentioned before. Our model allows to track and trace all of the information contained in the Blockchain. It also ensures that data has not been tampered with, bringing transparency, security and avoiding any kind of information manipulation. Consequently, we deal with grades' falsification, third party actions' fraud or malpractices. Additionally, with the use of Smart contracts to automate tasks, all the process speeds up, which allows for a more efficient procedure.

The structure of this paper is as follows. Section 2 explains in detail the concept of Blockchain and its main features. Section 3 presents the design of our theoretical approach. Section 4 presents the model by means of a simple example. Section 5 discusses the benefits and challenges of the proposed system and possible legal implications that the system entails. Section 6 concludes.

2. Blockchain Technology

Although Blockchain is most noteworthy in the financial sector, and, more specifically, to crypto currencies (e.g., Bitcoin, Ethereum, Ripple), its properties would allow us to

correct the weaknesses of the education system by doing it more reliable, allowing institutions and professionals to preserve their recognition and prestige.[5]

Blockchain can provide the education system with:[6]

- *Self-sovereignty:* "giving individuals the ability to be the final arbiter of who can access and use their data and personal information" (Camiller, 2017).
- *Transparency:* it is possible to give access to all parties so that any user can consult the information contained in the ledger in real time.
- *Immutability:* an immutable record is an unchangeable record whose state cannot be modified after it is created (Camiller, 2017).
- *Privacy*: only the receiver intended can read the message.
- *Integrity*: ensures that the information has not been altered by third parties.

Regarding *self-sovereignty,* the user is the owner of his or her own information. In terms of *transparency*, any user has access to the information available.[7] This will avoid malpractices as anyone can check all the information and can determine whether any user is favoring or damaging another. In terms of *immutability*, how the Blockchain technology stores information makes data immutable, since data is replicated across different Blockchains and a change in one location will be interpreted fraudulent and will therefore be rejected (Camiller, 2017). If, for instance, a member of the

[5] Although the blockchain definition that we use here does not consider tokens or currencies, some experts defend the need of monetary incentives for security reasons (Prisco, 2015).

[6] As Camiller (2017) points out "different blockchain implementations address these principles in different ways and to different extents. Not all the blockchains and/or the applications over different types of blockchains will embrace the entire set of principles underpinning the social value proposition of blockchain technology." We only focus on the properties of Blockchain that are especially significant in our model.

[7] In a permissioned ledger, the access to information will depend on the permissions acquired for the user. In a permisssionless ledger, all users have access to all the information (Rutland, 2017).

administrative staff wants to modify the scores of a student, he or she must modify that information in the corresponding block and has to modify it in all the subsequent blocks, making it very "expensive" in terms of effort and considered as fraud by the rest of the users. As for immutability, the Blockchain technology itself guarantees integrity of data. If a user wants to modify some piece of information, his or her acts will be registered in the ledger, being very easy to detect. This makes this technology trustworthy. In addition, Blockchain technology provides *privacy* for users. The user is invisible, putting aside gender or racial discrimination problems. However, this privacy can also be controversial (e.g., phishing and black markets). Finally, maybe the most important characteristic of Blockchain is *decentralization*. This means that there is no need for a central node to verify and supervise data. Therefore, users belonging to the network will be in charge of data verification. This is the most problematic property, and it requires the use of Blockchain technology (distributed ledger technology cannot avoid data manipulation) since although there is a consensus property, there is the threat of hacking the whole network.

Blockchain technology is present in a variety of educational applications. A majority of studies proposes Blockchain as a system to verify students' certificates.[8] EduCTX is a platform that is based in a decentralized distributed Blockchain that connects institutions to certify student's ECTS credits (Turkanović et al., 2018). It enables any institution to verify that any digital certificate in the possession of an individual is legitimate. In this way, paperwork and communication among institutions are reduced while simplifying the certificate management, storage and verification process.

[8] For a systematic review on Blockchain-based applications in Education, see Alammary et al., 2019.

There are some companies that are also introducing Blockchain to issuing certificates. One example is the company *Learning Machine,* which launched with MIT in 2016 an open source application named Blockcerts (MIT, 2018), recently joining Hylands. [9] Blockcerts allows institutions to issue digital diplomas that are in a Blockchain-anchored format, recipient-owned and instantly verifiable and shareable. Another example is Sony Global Education,[10] which is developing a platform to store, share and certify education and training data through Blockchain (*Sony, 2016)*. At present, it is using Blockchain technology to issue certificates at events such as the Global Math Challenge. Besides, Sony Global Education collaborates with the Japanese Ministry of Internal Affairs and Communications to demonstrate a next-generation school ICT environment. This project aims at securing the authenticity of transcripts and allow them to be safely shared within a trusted network.

Blockchain is also being tested in exams production. *DappER* is an application that produces exam papers within a permissioned Blockchain. The platform allows exams to be audited and reviewed in a decentralized and secure environment (Mitchell et al., 2019). Finally, one of the projects closest to our idea is developed by Lizcano et al. (2020), which proposes a model that certifies the acquisition of competencies of students using consensus protocol by means of teachers. In this way, they solved the difficulty that employers have in assessing students' skill level and to optimize their chances for future employability through the use of Blockchain technology.

[9] For further information, see https://www.hylandcredentials.com/ (last visited July 2, 2020)
[10] For further information, see https://blockchain.sonyged.com/ (last visited May 20, 2020) and https://www.sonyged.com/2016/02/22/news/working-on-the-blockchain/ (last visited May 20, 2020).

3. Model

Consider an institution that issues certificates.[11] In this institution, teachers are in charge of instructing the subject according to the contents of the syllabus and to employ the evaluation system stated in it.

There are students enrolled in this institution who attend classes, take exams, and review the results of tests to verify that the grade corresponds to the results obtained in the exams.

For simplicity, let us consider a single course, which is taught by several teachers, each of whom teaches the same course to different groups of students.[12] The framework considered can be described as follows:

1. The content of the course's syllabus is set by a national or supra-national institution (e.g., Department of Education). For the sake of simplicity, we assume that, to pass the course, students take only a final exam. This final exam will consist only of multiple-choice questions where the student's mastery of the entire content of the course will be evaluated.
2. The professor must follow the schedule that is set in the syllabus, so that all the content is taught and has been understood and assimilated by students.
3. After the teaching period, exams are carried out and will be automatically evaluated by Smart contracts. If the grade obtained is equal to or greater than 50%, students pass the subject.
4. After the exam corrections, there is a period of exam review in which students can check the mistakes they made.

[11] Depending on the institution considered, certificates may refer to either degree certificates or diplomas.
[12] The idea is to extend this method to all the courses required for the student to graduate in a particular field. More specifically, the idea is to spread this methodology to the rest of degree programs and institutions that belong to the network.

5. Students can ask for an in-depth revision to a committee of teachers. Once the exam has been reviewed, the score decided by the committee in charge of revising the exam, is transferred to the student's academic record.

3.1. The role of Institutions

In our model, institutions specialize in transmitting knowledge to students. Classes provide the material in a variety of different forms (Flipped Classrooms,[13] Smart Campus,[14] personalized and adaptive learning) to ensure students maximize their learning. In contrast to the actual education system, the teaching institution will not verify the student acquired knowledge. Certifications of the learning level acquired by students will be made using Blockchain technology and Smart contracts. Knowledge transmitter institutions belonging to the network of institutions interested in applying this decentralized methodology will agree on some objective criteria to measure the learning level the student end up with. We, therefore, do not propose a cyber-schooling system in which education is based on online tutoring and test-preparation and in which certification depends on the amount of time or the amount of work a student has submitted (Nespor, 2019).

3.2. Applying Smart contracts to Exams' Design

For exams' preparation, a computerized program can be designed containing the characteristics to be incorporated into the exam. In doing so, we can apply *Smart contracts*, which are self-executing agreements that reside in Blockchain or in Distributed Ledger Technology and that allow to automate and enforce a large number of processes in a safe and transparent way for all participants (Szabo, 1997).

[13] See (Bishop & Verleger, 2013) for a survey on flipped classrooms.
[14] See (Fernández-Caramés & Fraga-Lamas, 2019) for more information about smart learning and smart campuses.

A Smart contract refers not only to the computer code aspect, it also includes a legal piece, which reflects that the computer code constitutes a part of the binding legal agreement between the parties, i.e., the *contract* part. In the application of Smart contracts in exams, there are two different agreements to be considered. First, the one between students and teachers. Depending on the performance of the student during classes and during exams, the student can obtain a different score. Second, it is the one between students and institutions. Smart contracts can be used to establish the conditions under which a student receives a certificate from an institution and, therefore, when degree program's requirements are satisfied, and the student graduates. Smart contracts can also be used to link the achievements of a student in class and on the exam with the competencies and skills acquired with them. All of a student's achievements during his or her learning experience will be stored in a Blockchain-based wallet consisting of credentials that we call the "*student wallet*".[15]

3.3. The Role of the teacher

As a preliminary step, it is essential to explain in detail the role of teachers in this phase. In the current education system, teachers are in charge of the design of the course' program and of evaluating the learning process of students. If we just focus on teaching activity, we can summarize their tasks as follows: preparing classes, teaching courses, and setting, conducting, correcting and marking examinations. They are also in charge of reviewing examinations with students who wish to. The procedure ends up when teachers deliver grades to the administrative staff so that they are included in students' academic record.

[15] For more information, see Section 3.6. "The student wallet".

In our model, the teachers' role can be described as teachers, tutors or *coaches.* Teachers will be in charge of giving students all the tools to maximize their final grade. As Tapscott & Tapscott (2017) stated:

> *"The professors who remain relevant will have to abandon the traditional lecture*[16] *and start listening and conversing with the students. To begin, students could achieve the mastery of knowledge (anything where there is a right or wrong answer) by working with interactive, self-paced computer learning programs outside the classroom, freeing students and faculty alike to spend class time on the things that matter: discussion, debate, and collaboration around projects."*

In doing so, we will replace the more technical and routine teachers' tasks devoted to exam preparation, correction, revision and transmission by *Smart contracts*.

Hence, teachers' activities can be summarized in the following tasks:

- *Teaching:* teachers are required to teach the content included in the syllabus during the hours assigned by the institution, employing interactive and active learning. This also includes class preparation.
- *Office hours:* teachers must be available to students during office hours, which will be dedicated to solving students' uncertainties and to enable students to see concepts in greater detail.
- *Examination preparation:* teachers are required to prepare a certain number of questions for exams. Considering the content of the syllabus, each professor will propose a number of multiple-choice questions. For each question, the following information is also provided: options (*key* or correct answer and *distractors* or

[16] Tapscott & Tapscott (2017) describes the traditional lecture as the one in which "the teacher is the broadcaster and the student is the supposedly willing recipient of the one-way message".

incorrect answers), the solution of each question, and the level of difficulty of the question, which is also related with a previously specified learning level. Each question that the professor creates will also comprise a code indicating the epigraph of the syllabus that is evaluated with that question.[17]

- *BC-question ledger:* once teachers have created their questions, they are included in a Blockchain ledger (*"BC-question" ledger*), in which all of the information regarding the questions will be displayed.[18]
- *Question review:* In addition to preparing questions, teachers will review a specified number of questions that have been proposed by other teachers. To do this, teachers will use the questions included in the "BC-question" ledger, so that each professor will review whether the questions and answers are well written, if the solution proposed by the professor who has created them is the correct one and that the level of difficulty indicated is also correct.
- *Once the questions have been verified by a specified number of teachers, they can be selected to be included at the exam, being part of the "BC-exam" ledger, a ledger that contains the questions ready to be part of an exam.*

3.4. Exams configuration

We will use a Smart contract that selects the questions contained at the "BC-question" ledger to create exams and to certify a certain learning level. With this mechanism, a professor can customize exams, deciding the level of difficulty, number of questions, content of questions (by the epigraph code), restrict the use of questions only to those proposed by other teachers, employ the same exam for each group of students or create

[17] This is of application in the case that the syllabus of the course is sufficiently disaggregated to relate questions with specific sections of the units.
[18] We assume that teachers are the only ones allowed to propose questions (i.e., permissioned ledger).

a separate exam for each student while maintaining the same level of difficulty for all, among other possibilities.

In this way, teachers would save time, as exams would be created by a Smart contract that follows a series of instructions. In addition, given the large bank of questions in the "BC-question" ledger, it is very unlikely that a professor could provide the exam questions to students before the exam is held as the professor would not know which questions the Smart contract will select.

3.5. Conducting exams

When the exam takes place, the Smart contract is executed. After the examination, all of the information contained in the exam (questions and solutions proposed by the students) will be included in another Blockchain ("BC-evaluation" ledger) in which, applying again a Smart contract, exams will be scored based on the pre-determined correct answers. Finally, a grade will be assigned to every student.

The "BC-evaluation" ledger can be consulted by students and teachers, in such a way that it is not possible to know who has taken each exam.[19] If the student does not agree with his or her grade, it may be reviewed by several teachers of the subject, who will verify that the grade assigned is the correct one. Immediately after, that grade would be the valid one. Once the student accepts his or her grade (or after the review period deadline), the grade will be stored in what we call the "*student wallet*."

3.6. The student wallet

As we mentioned above, the student wallet is a digital wallet in which all the credentials of the student are stored after being awarded by any institution. The student wallet is not limited to the certificates that the student receives once a course is accomplished. With the use of Blockchain and Smart contracts, more information regarding the skills

[19] This ledger can be permissionless, in which case, anybody can consult the exams (parents, teachers, students, future or past students).

acquired in the completion of the course and the competencies acquired can be included. This is not only in relation with the new pedagogy concept mentioned above. With the system proposed and the existence of the student wallet, any student may have the possibility to customize learning by acquiring higher-level learning objectives in the skills that he or she wants. It is true that student efforts in a course depends on many issues, one of them being the expected utility the student obtains from a particular course (e.g., if Annie is studying Math but she is sure that when she graduates, she wants to specialize in Law, her effort level in Math is not going to be the same as for Jennifer, who want to specializes in Modelling). Students can attend similar courses but choosing the learning level they want to achieve, up to a minimum level required. When students are going to take the exams, they can select the learning level (also called the level of difficulty) and take exams based on that choice.

After exams are scored, students will receive in their student wallets the score, and a certification of the skills, and competencies acquired based on the learning level achieved.

The student is the owner of the student wallet, so he or she can choose which information to provide and to whom, whether employers or institutions. Essentially, students will decide to provide full or limited access to their student wallet. Besides, the student will know who is accessing this information, if the student requires the private key of the user to be revealed in order to consult certain information. Alternatively, the student can authorize anyone to access his or her wallet without identifying himself or herself.

4. An Example of a Simple Application

In this section, we explain in detail how the model could be applied by means of a simple example.

4.1. The "BC-question" ledger

For simplicity reasons, consider that three teachers are instructing the same course. Suppose that each of them has to prepare five multiple-choice questions for the course. For each question, each professor will prepare 4 possible answers, with only one of them correct. In addition, teachers would provide the level of difficulty[20] of the proposed question, according to the pre-agreed criteria. All these questions are uploaded at the "BC-question" ledger**,** a permissioned distributed ledger to which only teachers have access. Table 1 provides a visual example of the content included at the "BC-question" ledger.

	Content ID	Questions	All answers	Solution	Level of difficulty	Verification		Verified level of difficulty
						Prof. X	Prof. Y	
Professor 1	8.1	When…?	a,b,c,d,e	A	Easy	Easy	Difficult	Easy
	8.2	How…?	a,b,c,d,e	C	Medium	Easy	Easy	Easy
	8.3	What…?	a,b,c,d,e	B	Difficult	Medium	Medium	Medium
	8.4	How can…?	a,b,c,d,e	A	Easy	Difficult	Easy	Easy
	8.5	Is there…?	a,b,c,d,e	A	Medium	Easy	Difficult	Difficult
Professor 2	8.1	When…?	a,b,c,d,e	C	Difficult	Easy	Medium	Easy
	8.2	How can…?	a,b,c,d,e	A	Easy	Medium	Difficult	Medium
	8.3	Is there…?	a,b,c,d,e	C	Medium	Difficult	Difficult	Difficult
	8.4	When…?	a,b,c,d,e	B	Difficult	Easy	Medium	Medium
	8.5	How can…?	a,b,c,d,e	D	Easy	Easy	Medium	Easy
Professor 3	8.1	Is there…?	a,b,c,d,e	A	Medium	Medium	Difficult	Medium
	8.2	What…?	a,b,c,d,e	D	Difficult	Difficult	Easy	Difficult
	8.3	How can…?	a,b,c,d,e	D	Easy	Easy	Easy	Easy
	8.4	Is there…?	a,b,c,d,e	C	Medium	Easy	Medium	Medium
	8.5	What…?	a,b,c,d,e	B	Difficult	Medium	Easy	Medium

Table 1 A visual example of the "BC-question" ledger

[20] For simplicity reasons, we assume that there are three levels of difficulty (easy, medium, difficult), but more levels can be added.

After all teachers have proposed their five questions, each professor will verify that the questions proposed by the rest of the teachers are correct.[21] This means that teachers will verify that the questions and answers proposed by other teachers are well defined; the solution to the question is correct; and the difficulty of the question corresponds with the level of difficulty indicated by the professor who proposed it (see last column of Table 1) and with the learning level specified in the content of the syllabus. Once the question is verified by the rest of the teachers, the question is selected to be included in the "BC-Exam ledger," another permissioned distributed ledger in which all questions that are eligible to be part of an exam are included.[22]

4.2. The "BC-exam" Ledger and the Smart Contract for the Exam

The "BC-exam" ledger contains only those questions that have already been verified and that, therefore, can be included in an exam. The usefulness of the "BC-exam" ledger is more related to the exam design rather than the questions itself. In the exam ledger, a Smart contract[23] can be executed, indicating all of the characteristics of the exam and the contract between the student and the institution depending on the results obtained. For instance, the Smart contract of the exam can include the following features:

- Number of questions per level of difficulty
- Content of the questions
- Maximum number of questions proposed by the same professor
- General level of difficulty of the exam
- Exam content

[21] Given that there are 3 teachers in total, 2 will verify the questions of the other one, following a majority rule.
[22] Another option is to include all the questions in the same unique ledger but only questions previously verified may be used in exams.
[23] Depending on the features of the smart contract, this can be replaced by a self-executed software program.

- Exam date
- Skill or competency evaluated.

In Table 2, we depict how several questions are chosen following the instructions included in the Smart contract: four questions in total, no more than 3 questions per professor, level of difficulty: easy; content of the questions: one question per content (8.1., 8.2., 8.3., 8.4.).

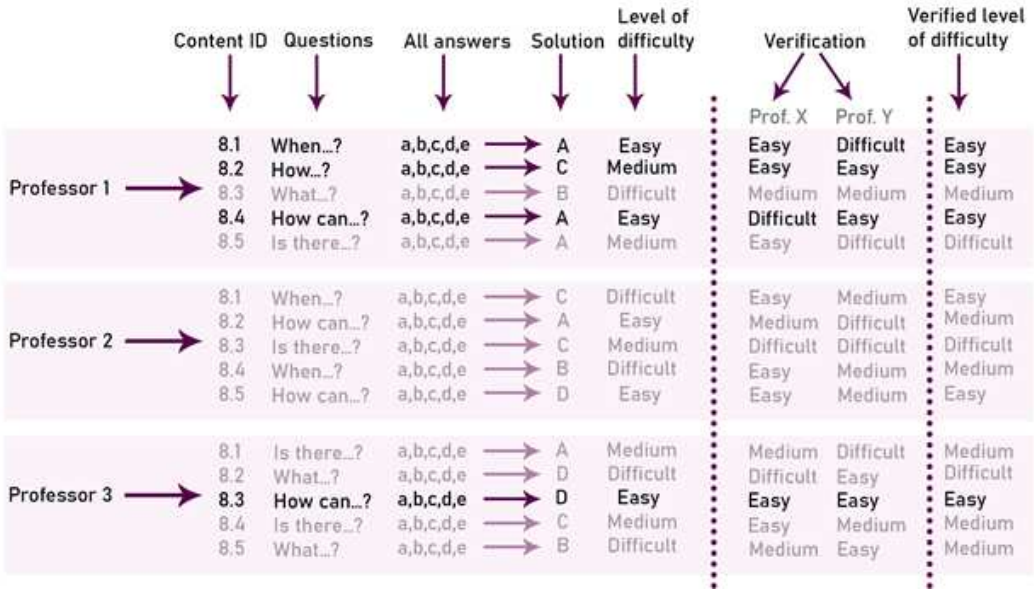

Table 2 A visual example of the "BC-exam" ledger when choosing questions.

Here, the possibility of customizing exams for students arises. For example, in the case of a student who wants to take an easier or a more difficult exam, he or she can select that option, which can be provided. Of course, the difficulty of the exam chosen will be also related to the learning level included in the skills acquired by the student and will also be recorded in the student wallet.

Once the exam is designed, the exam takes place on the scheduled date. Here, it is also important to provide how each question is scored (if incorrect answers are

penalized; if the weight of the questions on the exam is equal for all questions, among other issues). With these matters resolved, the overall grade obtained by each student can be calculated.

4.3. The "BC-evaluation" Ledger

The "BC-evaluation" ledger contains all of the information regarding students' exams. Table 3 depicts the content of this ledger. Each row contains each student's information. For example, row number 3 in Table 3 includes the information for Student 3, the level of difficulty of the exam (easy), his or her answers (C, B, C, B), the correct answer for each question (A, B, C, D), the grade obtained on the exam (5) and the score verified by all the teachers (5), except for the teacher who was in charge of Student 3 classes (Professor X).

	Questions	Level of difficulty	Q1 Answer	Q2 Answer	Q3 Answer	Q4 Answer	Q1 Solution	Q2 Solution	Q3 Solution	Q4 Solution	Grade	Verification			
												Prof. X	Prof. Y	Prof. Z	Student
Class (Prof. X)															
Student 1	Q1, Q2, Q3, Q4	Easy	A	B	C	C	A	B	C	D	7,5		7,5	7,5	7,5
Student 2	Q1, Q2, Q3, Q4	Easy	A	B	B	C	A	B	C	D	5		5	5	5
Student 3	Q1, Q2, Q3, Q4	Easy	C	B	C	B	A	B	C	D	5		5	5	5
Student 4	Q1, Q2, Q3, Q4	Easy	B	C	C	D	A	B	C	D	2,5		2,5	2,5	2,5
Class (Prof. Y)															
Student 1	Q1, Q2, Q3, Q4	Easy	A	B	C	C	A	B	C	D	7,5	7,5		7,5	7,5
Student 2	Q1, Q2, Q3, Q4	Easy	A	B	B	C	A	B	C	D	5	5		5	5
Student 3	Q1, Q2, Q3, Q4	Easy	C	B	C	B	A	B	C	D	5	5		5	5
Student 4	Q1, Q2, Q3, Q4	Easy	B	C	C	D	A	B	C	D	2,5	2,5		2,5	2,5
Class (Prof. Z)															
Student 1	Q1, Q2, Q3, Q4	Easy	A	B	C	C	A	B	C	D	7,5	7,5	7,5		7,5
Student 2	Q1, Q2, Q3, Q4	Easy	A	B	B	C	A	B	C	D	5	5	5		5
Student 3	Q1, Q2, Q3, Q4	Easy	C	B	C	B	A	B	C	D	5	5	5		5
Student 4	Q1, Q2, Q3, Q4	Easy	B	C	C	D	A	B	C	D	2,5	2,5	2,5		2,5

Table 3 A visual example of the "BC-evaluation" ledger.

One of the features of this ledger is that any student can consult his or her exam and the exam of any other student. By the Blockchain mechanism, the anonymity of the

students is kept safe and students are able to check whether exams were correctly scored, something students sometimes doubt.

Once the students revise their exams and accept their scores, it is automatically transferred to their students' wallets. If a student disputes the score assigned, he or she can ask for a revision. Given the exam design, students's claims are likely to be about exam content or the level of difficulty although the mechanism itself gives little room for this kind of mistakes. In any case, a committee consisted of external teachers can review their claims (see Teachers' verification columns in Table 3) by consulting the Smart contract code and the platform content. After teachers have verified the student's score, it will be transferred automatically to the student wallet.

4.4. A Smart Contract to Acquired Competencies and Skills

Another important task that can be designed by a Smart contract is to create a link between the content examined and the competence or skill acquired by the student. According to the Structure of the European Education Systems, programs from short-cycle tertiary education to Master's level are designed to provide skills and competencies leading to each degree qualification (Commission, 2018). Therefore, the design of the Smart contract in this case is of great importance since it involves the contract between the student and the institution in terms of skills and competencies acquired.

When the exam is taken, it is assumed that the student has acquired certain competencies or skills. Each exam provides not only the students' score in the course, it also provides evidence of the competencies and skills acquired by the student. Table 4 shows some competencies that can be evaluated in a course of Microeconomics. For example, if one of the questions requires the resolution of an economic analysis problem, the score obtained on this question will also address the student's economic

analysis competence (competence CE1 in Table 4). However, it is common to find only the final grade for the course on the student's transcript, with nothing about the competencies acquired by taking and passing the course or even the score obtained for each of the competencies. This can be driven by the complexity of linking competencies with knowledge acquired and, more importantly, with skills. Creating the contract is a great challenge as not all of the skills can be measured by a multiple-choice exam or by exams.[24]

COURSE	COMPETENCE CODE	COMPETENCE DESCRIPTION	SKILLS
Microeconomics	CG1	Autonomous and self-regulated work management	Independence
Microeconomics	CG2	Communication and information management	Communication
Microeconomics	CE1	Understand and interpret knowledge of key aspects of economic terminology, the nature of the economy and the immediate national and international economic environment	Economic analysis

Table 4 An example of some competencies evaluated in a Microeconomics course.

4.5. Student wallet

Finally, each student will find all the information about his or her courses taken, the scores, the competencies and the skills contained in a wallet. Table 5 provides an example of the information that can be contained in it. For instance, we can see all of the courses taken by the student, the institution in which the course is taken, the dates, the scores, the skills acquired (by means of a code that will also be included in the wallet), and the competencies by code.

[24] Although being out of the scope of this study, we should mention that evaluating competencies is a great challenge. This involves the ambiguity regarding the skill evaluated, the choice of activities to evaluate each competency by the teacher, how to measure, weight and evaluate each activity, among other aspects.

DATE	COURSE	INSTITUTION	SCORE	LEVEL OF DIFFICULTY	SKILLS	COMPETENCIES	VERIFICATION
Undergraduate Level							
December 2015	Microeconomics	U3CM	80/100	Easy	A1, A3, A4	C1, C3, C4	✓
February 2016	Statistics	Cambridge	60/100	Difficult	A8	C8	X
June 2016	International Trade	Standford	75/100	Medium	A4, A6	C4, C6	✓
September 2016	Public Law	Loyola	90/100	Easy	A1, A2	C1, C2	✓
Graduate Level							
October 2018	Advanced Statistics	MIT	70/100	Medium	A12, A13	C12, C13	✓
November 2018	Econometrics	UCLA	65/100	Difficult	A11	C11	X
December 2018	LATEX	Standford	85/100	Easy	A24	C24	X
Professional Level							
October 2019	SAP	U3CM	85/100	Easy	A15, A16	C15, C16	✓
December 2019	Professional english	Cambrigde	70/100	Medium	A18	C18	✓
January 2020	Latex	Cambrigde	90/100	Easy	A23	C23	X
March 2020	Chinese	HIT	60/100	Medium	A54	C54	X

Table. 5 The student wallet.

The student wallet will be owned by each student, who will give permission to the institutions to verify the information contained in it. Therefore, in the student wallet we can find two types of information, one that is already verified by the institution and another that is not (see last column in Table 5).

Any student is free to give access to his or her student wallet to any other user, including an institution or an employer to check his or her curriculum. With this methodology, the student will be the owner of his or her curriculum, avoiding typical situations in which the student spends money and time transferring the transcripts from one institution to another to, for instance, when enrolling in a master's degree program.

5. Discussion

5.1. Benefits and Challenges of the Proposed System

By using this design and evaluation system, the issuing institution, teachers and students obtain a multitude of advantages.

The system is fully transparent in the creation and assignment of grades. Teachers can verify the questions proposed by other teachers, the characteristics of the Smart contract, the examinations carried out by the students and their scores.

The students benefit the most. The system encourages teachers to make the most of the course and to teach classes as well as possible, in order to maximize both the highest possible number of students passing the exam and the highest average grade obtained, both signals of quality. When taking the exam, the learning level could be chosen by students, as specified in the Smart contract. In addition, as there is total privacy, no student will be able to be favored or harmed in the correction, enhancing equality and justice. In addition, students will be able to obtain the results of their exams once they finish, since a Smart contract or any other self-executing software will calculate the score, providing the credential in the student wallet immediately after student's verification of the grade. Additionally, the fact that each student can review his or her exam and the examination of other students makes this stage completely transparent, as it speeds up the review process and the inclusion of the grade in the student's record.

For the institution, the use of this system enhances its prestige, since the system is completely secure and impossible for students, teachers or administrative staff to engage in mis- or malfeasance. Besides, the speed with which grades are transferred to the student's academic record and the possibility that the academic record can be consulted by another institution would avoid students and institutions translating academic certificates, going through notaries, with the consequent loss of time that of all this entails. Besides, a system like this makes institutions compete to attract the best students and teachers. In fact, the typical argument that there are institutions in which it is easier to graduate than others will disappear, since all institutions belonging to the network will evaluate their students using the same evaluation methodology and difficulty levels.

Conversely, standard educational endeavors have a number of weaknesses that cannot be overcome by the proposed system. In the event that the students are low-skilled, regardless of the quality of teaching, students' test scores are not going to be the desired ones. Here, the key issue is the possibility to choose the level of difficulty for the examination to alleviate this type of situations and to adapt to the background of students.

One controversial issue is the fact that students can consult other students' exams. To what extent should they be given access to this tool? How could you prevent current students from leaking questions to future students? Would it be more appropriate to give access only to teachers?

Another of the drawbacks of the proposed system is the limitation to multiple choice questions only. We assume that with the use of *Smart contracts* and applying more complex designs, we could accommodate other types of responses, although, for the sake of ease, we continue to consider only multiple-choice questions.

For simplicity reasons, we have also assumed that there is only a final exam. However, this system can be applied with a continuous evaluation during the academic year by using a variety of tasks.

A final consideration would be whether there are other technologies that can be applied in this proposed system that are more effective or efficient. In this sense, it is important to consider whether the use of a distributed ledger is sufficient to satisfy all the properties of security and trust or whether Blockchain technology is needed. Similarly, to what extent smart contracts are needed or whether self-executed software programming is sufficient to validate results. In any case, the level of decentralization will determine these specifications.

5.2. Legal Implications

In this section, we focus on the legal implications that arise from the proposed system. We briefly examine the issues that can arise with personalized learning, the level of difficulty and learning level setting, the possibility of breaking contracts between students and institutions, and identity fraud, among others.

- *Is it legal to discriminate for students' level? Which method can be used to avoid discrimination externalities?*

The fact that a student can choose the learning level for a course or a skill allows students to customize their curriculum and exams. Although students can choose the learning level they want to achieve, the use of different levels of difficulty for each learning level in evaluating exams can be considered discrimination. Knowing the type of student and designing the exam depending on his or her capabilities, especially in the case of special needs, will be a good way of encouraging students to maximize their level of effort while having them make the most of the course. However, it can be unfair to permit different levels of difficulty for different students. In order to deal with it, exams should be designed in the appropriate way so that any type of student is not penalized by different types of exams. Besides, this difference in the level of difficulty has to imply differences in the curriculum. That is, if a student chooses a higher level of difficulty, these should be included in his or her wallet.

A possible example in which this can be solved is as follows. For a 10 multiple-choice question exam, 5 questions are of low level, 2 questions are of medium level and 3 questions are of high level. Depending on the number and type of correct answers, the mark of the student will be different. In this way, there is no discrimination since students with low motivation or low capabilities in the course can pass the exam (although it is very much more difficult for them to get a higher mark).

- *Minimum learning level required to pass a course*

Another issue is who will set the level of difficulty required to pass a course. In a centralized system, a higher institution (e.g., Department of Education) can set the requirements to pass a course and relate the level of difficulty of an exam to a certain learning level acquired. In a decentralized system, teachers are the ones setting these levels. Which method do they use to reach an agreement? Which majority rule can be used to make these decisions? In terms of setting a majority rule, a simple majority would be enough. However, setting the level of difficulty for an exam will be the most controversial as it could be considered to be subjective.

- *"Right to forget"*

Blockchain technology will preserve all of the information regarding any student and any professor. Is it legal that all of the information of a student is released to employers, companies, and other users? Can the user decide which information can be consulted from her public profile? We assume that the proposed *student wallet* will be a seamless solution for this problem, since the student is the owner of their credentials (self-sovereignty) and the institutions are only playing a role in issuing the certificates that are included in the student wallet. However, the amount of information a student decides to make public in his or her student wallet can also be used as a signal of his or her type. It is possible that a student only give access to his or her credentials in those competencies or skills in which his or her performance was higher. All the information that is not published can be understood by employers as a way of hiding low results. Therefore, the premise that the student is the owner of his or her own student wallet and that he or she can choose what to publish is not so clear since those not publishing everything can be disregarded by employers due to this lack of transparency.

- *Identity fraud? Need of companies that certify the identity of exam holders and the use of Multisig Technology*

Our proposal allows any user to take the exam anywhere. However, it is of vital importance to ensure that the students taking exams corresponds to the user they are "telling" they are. In doing so, there are two different solutions. First, an appeal to companies that certify the identity of the user taking the exam. Another system will employ the use of biometrics, together with Multisig technology (a combination of several keys can be required instead of one single private key).

- *Academic property rights: What are the implications of being the owner of your own certificates?*

In the current system, students earn their certificates after completing all of the courses. However, often a student contacts the issuing institution to ask for transcripts or to require other kind of certificates that certify that the student has completed a course. With the student wallet, we propose a system in which students do not need to spend time and money on doing this task anymore. But what implications does the student wallet have? Can wallet information be stolen? Again, identity and authenticity measures have to be taken to guarantee the correct use of this particular Blockchain.

- *Breaking contracts*

The contract between the institution and the student can be broken in several respects. To mention some, if teachers cannot complete all the course, or if the level of difficulty of the exam is not correctly specified with the learning level in advance. In both cases, students can claim that the exam results have been corrupted by these anomalies and have the right to ask for compensation. The matter in question is what the fair compensation for a student in a situation like this is.

- *How legal would it be to have a decentralized institution issuing certificates?*

The system that we propose can also issue certificates to those users that have passed the exams. To what extent is it legal that a decentralized system like the one that we propose be authorized to issue certificates? What are the implications for other institutions? This is one of the most important implications that this system can infer, since it will enter into conflict with the actual system in which institutions compete for students and their supply of degrees, its prestige and its location set students' preferences to apply for one or another institution. With our proposal, the validation of the certificate issued will be the first step to overcome. As a first step, we believe that the authority in this system can be distributed among a set of trusted organizations (institutions belonging to the network). This is a step towards what Charles M. Vest defined as the Meta-University: *"a transcendent, accessible, empowering, dynamic, communally constructed framework of open materials and platforms on which much of higher education worldwide can be constructed or enhanced"*(Vest, 2006).

6. Concluding remarks

The latest technological advances have allowed the application of Blockchain technology and Smart contracts in sectors other than finance. Its properties of self-sovereignty, transparency, privacy, immutability and integrity make desirable the introduction of Blockchain in any sector in which there are exchanges of information and where information manipulation is possible.

The introduction of this new technology in the education sector enhances efficiency and efficacy, while generating equality and fairness at higher levels of education. On the one hand, it is possible to reduce waiting times in different activities (e.g. from the exam realization until grades are published). It also reduces working times, avoiding duplication of activities (e.g. when different teachers have to prepare different exams for

their groups and for the same course). Finally, the major contribution of Blockchain technology is that it would make unnecessary the participation of a central intermediary to verify information, as the technology itself will do so.

The application that we propose is still novel and is not in use yet. All the advantages that we mention in terms of enhancing the prestige of institutions and teachers, time efficiency, the possibility to customize student education and the use of a student-owned wallet, are worth enough to overcome all the challenges still needed to be faced. Undoubtedly, the next step is to validate the model by means of a simple prototype to be aware of the weaknesses and the applicability of the model itself.

It is also noteworthy to mention the implications in terms of legal aspects with regards to privacy, discrimination and academic property rights, that must be carefully considered in the development of this technology. Most importantly, an open environment like the one we propose will require the application of the same law and the definition of a virtual jurisdiction in which no one can be benefited nor damaged. Smart contracts itself are also problematic. To mention some, the contracting parties are not the only ones participating in a contract. The creator of the contract and the designer of the contract can also have responsibilities. The absence of a virtual jurisdiction can make contract creators and designers free of charge.

Finally, the use of Blockchain as a source of trusted identity would represent a major step toward the recognition of Blockchain as an immutable source serving as a valid legal tool for issuing information such as certificates. Overcoming the complexity of the technology itself while considering the legal implications and challenges of its use are the key to start benefitting from all its rewards.

References

Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-Based Applications in Education: A Systematic Review. *Applied Sciences*, *9*(12), 2400. https://doi.org/10.3390/app9122400

Bishop, J. L., & Verleger, M. A. (2013). The flipped classroom: A survey of the research. *ASEE Annual Conference and Exposition, Conference Proceedings*.

Blockchain | Definition of Blockchain by Merriam-Webster. (n.d.). Retrieved July 2, 2020, from https://www.merriam-webster.com/dictionary/blockchain

Camiller, A. G. A. F. (2017). *Blockchain in Education Luxembourg : Publications Office of the European Union*. https://doi.org/10.2760/60649

Commission, E. (2018). *The Structure of the European Education Systems 2018/19: Schematic Diagrams*. https://doi.org/10.2797/302115

Digital Credentials | Hyland Credentials. (n.d.). Retrieved July 2, 2020, from https://www.hylandcredentials.com/

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2019). Towards next generation teaching, learning, and context-aware applications for higher education: A review on blockchain, IoT, Fog and edge computing enabled smart campuses and universities. *Applied Sciences (Switzerland)*, *9*(21). https://doi.org/10.3390/app9214479

Lizcano, D., Lara, J. A., White, B., & Aljawarneh, S. (2020). Blockchain-based approach to create a model of trust in open and ubiquitous higher education. *Journal of Computing in Higher Education*, *32*(1), 109–134. https://doi.org/10.1007/s12528-019-09209-y

MIT. (2018). *Blockcerts : The Open Standard for Blockchain Credentials*. https://www.blockcerts.org/

Mitchell, I., Hara, S., & Sheriff, M. (2019). dAppER: Decentralised Application for Examination Review. *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 1–14. https://doi.org/10.1109/ICGS3.2019.8688143

Nespor, J. (2019). Cyber schooling and the accumulation of school time. *Pedagogy, Culture and Society*, *27*(3), 325–341. https://doi.org/10.1080/14681366.2018.1489888

Prisco, G. (2015). *Circle's CEO Jeremy Allaire Defends the Bitcoin Blockchain*. https://bitcoinmagazine.com/articles/circle-s-ceo-jeremy-allaire-defends-the-bitcoin-blockchain-1447173474

Rutland, E. (2017). *Blockchain Byte*. http://www.finra.org/sites/default/files/2017_BC_Byte.pdf

Sony Global - Sony Global - Sony Global - Sony Global Education Develops Technology Using Blockchain for Open Sharing of Academic Proficiency and Progress Records. (n.d.). Retrieved July 2, 2020, from

https://www.sony.net/SonyInfo/News/Press/201602/16-0222E/

Stephen Burgen. (2018). *Fake degree claims dog prominent Spanish politicians | World news | The Guardian*. https://www.theguardian.com/world/2018/apr/10/spanish-politicians-urged-to-resign-over-fake-degree-claims

Szabo, N. (1997). *The Idea of Smart Contracts*. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

Tapscott, D., & Tapscott, A. (2017). Higher Education The Blockchain Revolution and H igher Education. *Educase*.

Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access*, *6*, 5112–5127. https://doi.org/10.1109/ACCESS.2018.2789929

Vest, C. M. (2006). Open Content and the Emerging Global Meta-University. *Educause Review*, *41*(3), 18–30. http://www.educause.edu/apps/er/erm06/erm0630.asp