isla
instituto politécnico de gestão e tecnologia

ISLA
Santarém

MESTRADO EM ENGENHARIA DE

TECNOLOGIAS E SISTEMAS WEB

BLOCKCHAIN AND REMOTE ASSESSMENT SYSTEM

A conceptual approach for plagiarism mitigation in the Higher Education Institutions

Paulo Victor Guerreiro Ferreira Dias

Prof. Dr. Firmino Silva

DISSERTAÇÃO

VILA NOVA DE GAIA

09 | 2022

Dissertação de Mestrado realizada sob a orientação do Prof. Doutor Firmino Silva apresentada ao ISLA - Instituto Politécnico de Gestão e Tecnologia de Vila Nova de Gaia para obtenção do grau de Mestre em Engenharia de Tecnologias e Sistemas Web, conforme o Despacho n.º ……..

INSTITUTO POLITÉCNICO DE GESTÃO E TECNOLOGIA

BLOCKCHAIN AND REMOTE ASSESSMENT SYSTEM

A conceptual approach for plagiarism mitigation in the Higher Education Institutions

PAULO VICTOR GUERREIRO FERREIRA DIAS

Aprovado em 18/10/2022

Composição do Júri

_____

Presidente (Prof. Doutor Jorge Pereira Duque)

_____

Arguente (Profª. Doutora Paula Peres)

_____

Orientador/a (Prof. Doutor Firmino Silva)

Vila Nova de Gaia

2022

Acknowledgment

In these last years of hard study, I would like to thank all the people who were fundamental for the realization and conclusion of my master's degree.

I would like to express here, in a few but very sincere words, a little of the relevant role they played in my achievement.

My special gratitude goes to Prof. Dr. Firmino Silva, my advisor, for his excellent professionalism and for the human being of great value, who embodies in himself a particular and differentiated sense. Likewise, thank ISLA Institute for offering all the academic conditions for the realization of a master's degree of unquestionable quality.

I also thank all the other professors who contributed to the enrichment of my knowledge during the course of this master's program.

A fraternal thanks to all my classmates for the direct and indirect support in my graduation, now, as a master in engineering.

Once again, thank you all for the teachings, companionship, and for the friendship that we have built over the years. Without this strength, this achievement would certainly not have been possible.

ABSTRACT

DIAS, Paulo Victor Guerreiro Ferreira. *BLOCKCHAIN AND REMOTE ASSESSMENT: A conceptual approach for plagiarism in the Higher Education Institutions*. 86p. Dissertation (Masters in Engineering of Technologies and Web Systems) – Polytechnic Institute of Management and Technology, Vila Nova de Gaia, 2022.

The realization of remote assessment, supported by Information and Communication Technologies, is an issue of great concern for Higher Education Institutions. Phenomena of fraud and plagiarism are frequent, difficult to detect and reached high values during the Covid-19 pandemic. Although tools that mitigate these practices already exist, these phenomena still represent a barrier to the full execution of distance assessment elements. This research work proposes to develop, through knowledge of the state of the art, a technological framework that involves components that can address the difficulties in which the remote assessment process relies. Plagiarism detection tools, Digital Signature principles and Blockchain are analyzed as potential components of the framework and that may constitute a new approach in mitigating or eliminating the use of plagiarism or e-cheating factors in remote assessments. These factors are identified, aggregated, and classified in order to be addressed by the technological components of the framework. The main objective of the framework is to contribute to the improvement of information security and reliability in the assessment system in distance learning in Higher Education Institutions.

Keywords: Blockchain, Plagiarism tools, Digital Signature, HEI, e-Learning, Remote Assessment.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AR	Augmented Reality
CA	Certification Authorities
DSR	Design Science Research
HEI	Higher Educational Institutions
ICT	Information and Communication Technologies
IDE	Integrated Development Environment
IoT	Internet of Things
IS	Information Systems
LMS	Learning Management System
MOOC	Massive Online Open Course
OECD	Organization for Economic Co-operation and Development
P2P	Peer-to-Peer
PKI	Public Key Infrastructure
PoS	Proof of Stake
PoW	Proof of Work
RA	Registration Authorities
SMOC	Synchronous Massive Online Course
SPOC	Small Private Online Course
SSOC	Synchronous Small Online Course
UNESCO	United Nations Educational, Scientific And Cultural Organization
VR	Virtual Reality
WHO	World Health Organization
XR	Extended Reality

SUMMARY

1. INTRODUCTION

This chapter is intended to present the context and motivations of this dissertation, the problem definition and the objectives to be attained, and the research question and methodology around the subject in question.

1.1. BACKGROUND

The digitalization progress is a process increasingly present on the day-to-day life of businesses and people and it will pervade all areas of the economy, causing multiples economic and social transformations in the next years [1].

A countless number of devices capable of communicating with each other and collecting environment and user's data (e.g., smartphones, vehicles, appliances, illumination systems, etc.), associated to big data technologies, cloud computing and new data management technologies, certainly will broad space for new business models to be created ([2], [3], [4]).

The way business relate with clients and suppliers is going through fundamental changes, with all being addressed as part of the Industry 4.0 [5]. A decade ago, PwC (PricewaterhouseCoopers) started a study analyzing more than 250 emerging technologies [6], in a way to find out what would be the ones with the most impact across industries. This study culminated in what they called Essential Eight, composed by Artificial Intelligence (AI), Augmented Reality (AR), Blockchain, Drones, Internet of Thing (IoT), Robotics, 3D printing and Virtual Reality (VR). Nowadays, these technologies continue to evolve, with most of practical and profound impact coming from them in the next five years. Their combination can reconfigure these tools into different approaches. One way is automating trust, mixing blockchain, IoT and AI, to ensure the authenticity of data, verify identities and enable secure multiparty transactions. Another way would be the extended reality (XR), combining AR, VR and mixed reality (MR) to bring new customer experiences, to speed up product development and also improve workspace safety. Others power combinations can also make a big impact, such as immersive interfaces (using senses and other perceptions to interact with technologies), working autonomy (integrating automation, robotics and intelligent systems to transition manual to digital processes), and hyperconnected networks (IoT and network infrastructure to process information at blistering speeds to connect people, devices and systems in an intelligently way).

These changes can already be seen on full speed in sectors like computing and automotive, but a countless number are still lagging out [7]. Regarding the Educational Sector, several, but shy on engagement, initiatives were being created to bring the so traditional field to a more digital world. Online systems such as Moodle or other Learning Management Systems (LMSs) are broadly used in the Higher Educational Institutions (HEIs), but mostly for calendar

control, communication between the HEI or lecturer and their students and sharing documents and assignments ([8], [9]). Then, e-learning platforms gained popularity with asynchronous classes on Massive Online Open Courses (MOOCs) formats, but struggled to gain traction as the motivation of students decay over time, ranging from 2 to 10% of the students completing a course on average ([10], [11]).

1.2. MOTIVATION

On March of 2020, the World Health Organization (WHO) declared the outbreak of COVID-19 pandemic [12]. Overnight, personal contact was forbidden, traffic around cities and countries either, and besides hospitals and other essential services, all business doors were shut. As a result of that, a whole new set up of how businesses and people relate were immediately demanded. Remote conferences gained extremely significance, with a boom on Zoom calls and other akin [13]. Other services that were still crawling in adoption, such as telemedicine, e-commerce, food delivery also spiked rapidly [14].

Schools and HEIs were directly affected with the traffic restrictions [15], indoor classes were not possible anymore and business rushed to improve or develop online tools and platforms to meet this demand. As the pandemic still remains, this reality has opened new opportunities in the definition of teaching strategies. Exploiting the advantages of this teaching modality, classes with theoretical content, with less or no use of laboratory practice, are already commonly guided by technologies that support e-learning.

Given the aforementioned overview of the current eLearning systems, it becomes crystal clear that what the existing platforms could embrace was not enough for what the transformation of the sector, accelerated by the COVID-19 pandemic, was demanding for. Global mobile learning is expected to grow from $22.4 billion in 2020 to $80.1 billion by 2027 [16].Therefore, key aspects of improvement of the eLearning system seems to have a powerful synergy with blockchain technology. With more individuals being part of distance learning, a considerable amount of personally identifiable information is transmitted between the student, the institution, and third-party suppliers as part of the educational or training process. This brings the need for a system that can combine information security and the ability to send data across a big network in a purely virtual manner. And for that, blockchain appears to be tailor-made to assist in safeguarding and protecting this new model of education [17].

1.3. PROBLEM DEFINITION

Although it is not desirable to have this method of teaching covered in all teaching stages, namely considering the evaluation moments, there are circumstances in which, for reasons of reduced student mobility or health safety, it becomes the only possible way to contemplate the student's evaluation process.

Since all these modality changes were demanded in short term, communication, collaboration, and exchange of information were the focus of this first step of digitization of the schooling. Now, on a second term, safety and authenticity have raised concern [18].

This vicissitude has created enormous challenges for distance assessment models, especially in higher education. The reliability of a distance assessment system has deserved the attention of the scientific community, which addresses, on one hand, the definition of assessment strategies, and on the other hand, the adoption of technologies that promote a high degree of integrity of the distance assessment system [19].

1.4. RESEARCH QUESTION

This research work aims to analyze the application of a blockchain framework in the process of reliability and validation of information exchanged between students and educational institutions, such as the assessment level, in order to mitigate plagiarism or e-cheating factors.

The research question of this work is the following: "**How can a blockchain-based framework support an assessment strategy in higher education, mitigating or eliminating the use of plagiarism or e-cheating factors?**"

1.5. OBJECTIVES

Potential issues to be raised gravitate around the authenticity of information provided by the student in online activities, such as remote assessments, use of smart contracts [20] in the academic environment, mitigation of plagiarism of papers, copyright, authenticity, integrity and immutability of academic documents.

Given the aforementioned concerns, the objectives of this research can be broken down into the following main goals:

- Studying and raise the methods of the state of the art of distance learning in the higher education to better understand the current procedures and frameworks to reduce e-cheating in the HEI's environment;
- Identifying the main guidelines used to mitigate plagiarism on the e-learning environment of the HEIs;
- Definition of requirements to define a framework, based on blockchain, that will assist on the interaction between students and HEIs during assessments;
- Identify the blockchain network model for validating the information between students and educational institutions;
- Build a prototype of a blockchain system to test the studied concept;

- Contribute to the improvement of information security in the distance learning system in higher education.

1.6. HYPOTHESIS

Given the continuity of the actual pandemic, and bracing itself for potential other that may arise in the future, this research work relates to some hypothesis that already seems to be in motion, namely:

- the distance learning model become the standard for teaching, namely in the theoretical programmatic contents;
- all theoretical assessments can be done in digital mode, with total security of authenticity, avoiding e-cheating and plagiarism.

1.7. METHODOLOGY

To assure the rigor and relevancy of this proposed work, a solid method of research becomes necessary for both academic field and society in general so it can have its results easily accessed, checked, and be subject to discussion and verification.

As defined by Hevner et al. [21], design science research (DSR) is a research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artifacts, thereby contributing new knowledge to the body of scientific evidence. The designed artifacts are both useful and fundamental in understanding that problem.

When we bring this to context, there are two distinct, but complementary, paradigms for Information Systems (IS) research which are Behavioral Sciences and Design Sciences. The first, which has its origins from natural science, starts with a hypothesis, then researchers collect data, and either provide or disprove the hypothesis, and eventually a theory gets developed. The latest, on the other hand, is fundamentally a problem-solving paradigm whose end goal is to produce an artifact which must be built and then evaluated.

Using Hevner's design science research cycles, Figure 1, as base to develop this research will bring robustness to the whole process. In this method, several activities are combined in three cycles, namely the Relevant Cycle, the Rigor Cycle and the Design Cycle [21].

Relevance Cycle. It often begins by identifying and representing opportunities and problems in an actual application environment. This application consists of people, organizational systems, and technical systems that interact in order to a goal. Two questions underlie this cycle: *does the design artifact improve the environment* and *how can this improvement be measured*? The output must be returned into de environment for study and evaluation in the application field. The outcome of the field testing will specify if additional iterations are needed.

Rigor Cycle. Responsible for building up the basis for the scientific knowledge of the research. It combines the experiences and expertise that define the state of the art in the application domain with existing artifacts and processes also found in the application domain. This way, it provides past knowledge to ensure the innovation of the research project.

Design Cycle. This is the central part of the design science research project. It is where the artifact is conceived, maintaining the balance between the relevance cycle – where requirements are settled – and the rigor cycle – where the knowledge and groundings are built.

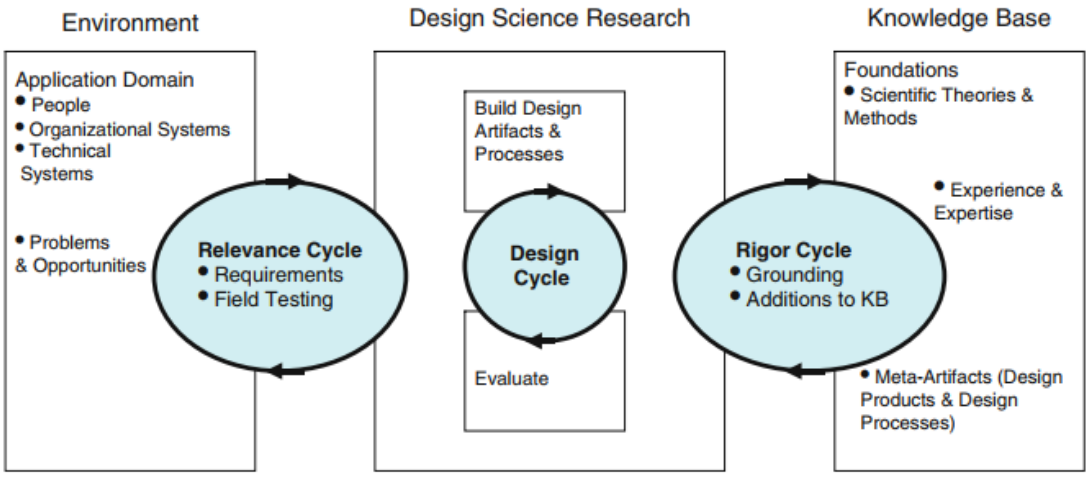

Figure 1 *- Design Science Research Cycles [21].*

This dissertation's research approach follows a design science method described above, which is based on the creation and validation of IT artifacts with the purpose of solving organizational problems. The proposed framework in this research project represents the actual artifact, supporting a system to analyze the application of blockchain in the process of reliability and validation of information on the HEI environment, comprising specially at the assessment level, in order to mitigate plagiarism and/or e-cheating factors. As described above, three components of interaction between design science and behavioral science are identified: the environment, information system research, and knowledge base. These components are used as a foundation for the structure of this research work.

Table 1 indicate the methodology used in this research work splitting the main steps into 4 parts: A) Identification/Definition of the theme and environment research; B) Literature review/Related work; C) Framework development; D) Validation; and E) a fifth final extra step related to completing the writing of this dissertation.

The table correlates each step mentioned above in the Design Science Research framework of Hevner et at. [21]. Firstly, the environment is set up (Step A). Then, a substantial literature review is presented (Step B) in order to build the proposed framework (Step C). Additionally, the knowledge base is used as a

basis to build the artifact – *Conceptual Framework* –, and also used to provide methodologies for the validation step (Step D). The process is iterated several times to enhance the conceptual framework. The next section identifies how the chapters of this thesis are structured.

Table 1 *- Addressing used methodology to Hevner et al. [21] DSR framework.*

Hevner et al. [21]: DSR framework	Methodology	Dissertation index
	A. Identification / Definition of the research theme and evironment	
Enviroment - Identification of Problems & Opportunities	A.1 Framing environment	1.1 Background 1.2 Motivation
Relevance Cycle - Identification of Requirements	A.2 High-level requirements definition	1.3 Problem Definition 1.4 Research Question 1.5 Objectives 1.6 Hypothesis
	B. Literature review / Related work	
Knowledge Base - Grounding / Foundations	B.1 Distance learning and blockchain related to the educational sector	2. Literature Review
	C. Framework development	
Design science - Build design artifacts & processes / Design Cycle	C.1 Artifact design	3.1 Stakeholders 3.2 Framework
Rygor cycle - Additions to Knowledge Base / Design Cycle	C.2 Framework contribution	3.3 Implemenation
	D. Validation	
Design science - Validate / Design Cycle	D.1 Artifact validation	3.3.4 Testing
Relevance Cycle - Field Testing		3.4 Cost Analysis
	E. Completing writing the Master Dissertation	

1.8. DISSERTATION STRUCTURE

The dissertation is composed of 7 chapters, comprising from Introduction (Chapter 1) to Future Work discussion (Chapter 7). Each chapter is supported by the previous one, creating a comprehensive and structured description of the research.

In a nutshell, Chapters 3 and 4, which are devoted to develop and implement the conceptual framework (the artifact), have its groundings in Chapter 2. Chapter 5 discusses about alternatives and privacy and security measures regarding what was presented in the previous two chapters. Based on all these chapters, Chapter 6 considers the obtained results and Chapter 7 details possible improvements. Below, each chapter have its content detailed.

In Chapter 2, the related work with the main guidelines of this research is analyzed. Different tools regarding authenticity methods and security of the information are discussed. Also, a comprehensive analysis of existing frameworks destined to distance learning and their challenges is made. Then, the concepts surrounding blockchain are detailed and its applicability to the Educational Sector, especially in the Higher Education, are exposed.

Chapter 3 conceptually discusses the architecture supporting a framework solution to enhance the authenticity and integrity of the remote assessment process in a HEI. The elements of each level and the interactions between the elements are described, as well as the functioning of the smart contracts and their interoperability.

In Chapter 4, the framework is validated in a controlled scenario and a cost estimative is presented.

In Chapter 5, possible alternatives are discussed regarding types of blockchain, their validation systems, and other aspects. Privacy and security matters are also a topic that are detailed towards the developed framework.

In Chapter 6, the conclusions of the dissertation are presented.

In Chapter 7, the directions for future research work are presented.

2. LITERATURE REVIEW

This chapter covers the state-of-the-art of the topics outlined in the Introduction chapter.

Section 1.5 brought to light what is intended to be achieved by the end of this research work. These objectives include the development of a blockchain framework to validate a new way of exchanging sensitive information in the educational field complying with the authenticity, immutability and security of the information.

Therefore, the sections ahead depict the state-of-the-art of the most up-to-date topics, including digital signatures and cryptographic methods, the progress of e-learning platforms utilizing blockchain as base (emission of certificates, educational passports, universal credit systems, etc.), and other frameworks geared towards data protection and antiplagiarism using blockchain.

2.1. DISTANCE LEARNING IN THE HIGHER EDUCATION

According to OECD [22], e-learning refers to the use of Information and Communication Technologies (ICT) in diverse processes of education to enhance and/or support learning in tertiary education. This comprises ICT in four different manners: web-supplemented, focused on classrooms but including elements such as e-mail and online links for extra resources; web-dependent, where it requires the students to interact in online discussions or collaborative work without reducing classroom time; mixed mode, with part of classroom time being replaced by online graded activities; and fully online, where students can attend the whole course without the need of physical presence.

Nowadays, this dynamic has evolved from what was once the transition from in-person to remote learning to a new phase where engagement, online experience and retention of the students became the next in line. Covid-19 crisis has a big part in pushing the urge for change on the way e-learning should be. Heitz et al. [23] propose some specific actions that HEIs could take to enhance their capabilities of online instructions: focus on access and equity, support to faculty members, move the stakeholders to the online environment and encourage their interconnections, and invest in cybersecurity.

2.1.1. Overview of Existing Frameworks

This section explores some existing frameworks for e-learning and the different ways online teaching are arranged. Also, a specific look into the remote assessment's challenges is discussed. Distance learning brings new perspectives for tutoring. As well as being separate by physical space, distance learning students also can be separated by time. This time separation is split into two categories: synchronous and asynchronous [24]. Synchronous refers

to a real-time method of education, using video conferences and other types of online communication technologies to achieve this. On the other hand, on asynchronous distance learning, students are able to go through the course program on their own pace, with the content recorded in some online platform. Usually, it has a limited time spam for completion of the assignments, but students are free to work at their own speed [25].

Kaplan et al. [26] defines and classifies distance learning, elucidating the types that are used. Massive Open Online Course (MOOC) is an online course that provides active elements to support interactions among students and allows unlimited participation. In contrast, Small Private Online Course (SPOC) offers limited number of students and requires formal enrollment, frequently charging some tuition fee. These definitions, according to Kaplan, can be classified in two dimensions: number of participants and time dependency. MOOCs enables students to learn on their own pace without the need to stick to a schedule. Similar, Synchronous Massive Online Course (SMOC) also allows the participation of unlimited students, but requires their presence at the same time, usually assisted by videoconference platforms. With similar aspects but with limited participants, the term Synchronous Small Online Course (SSOC) is used.

All these distance learning definitions and methods mentioned above needed to be materialized into some digital platform. Learning Management Systems (LMS) were created for this purpose. An LMS enables the management, student monitoring, tracking of learning, communication, integration of multiple media, and presenting all of it in an organized manner ([27], [28], [29]). Cavus [27] highlights some common features of LMSs, such as the delivery of knowledge in various forms (MS Office, video, audio, etc.); assessments via homework and examinations; communication between student-student and student-teacher; class management, and others. LMS on the market vary in many forms depending on the goal of the institution that is intending to use it. It can be obtained for free, such as Moodle, ATutor, etc., or throughout payment – Blackboard, WebCT and others [30]. As part of UNESCO's covid-19 education response, a very complete list of several educational applications, platforms and resources were made available in their website. It covers areas like psychosocial support, digital learning systems – with ones destined to basic mobile phones and offline content to facilitate access to less resourceful people – MOOC platforms, self-directed learning content, tools for teachers to create digital learning content, and repositories [31].

Although the abovementioned platforms were responsible for a great step into a more democratized access to education and to the spread of knowledge in the modern world, they still have problems regarding some aspects in terms of credibility, credit certification and certificates, and student privacy. This way, in the past few years, blockchain technology have been put into test in most various ways as a possible solution for future online education.

Oganda et al. [32], through cases studies and the development of a Business Model Canvas, provided the results of integrating blockchain technology with the MOOC-based Smart Program Education platform – *Education Smart Courses (ESC)*. The Business Model Canvas on ESC consists of nine basic components of the business model, comprising on the left side related to products, the market on the right, while the value proposition is divided into half. Figure 2 illustrates the canvas model. Conclusions of the authors of [32] this research work points out that mixing blockchain with MOOC platforms could become a trend. The ability to create cryptocurrencies by blockchain might find significant use in grants and/or voucher-based education funders in many countries. Other main advantage is that provides a safe record of teaching, available and decentralized for many teachings.

Lam and Dogol [33], also in the same direction, goes further on combining blockchain with e-learning platforms. In their paper, it is introduced a proof-of-concept blockchain-based e-learning platform, called Blockchain University, developed to increase transparency in assessments and facilitate curriculum personalization in the higher educational context. The authors designed their case to be pedagogically neutral and content-neutral in order to showcase the benefits for both end users such as students and teaching staff. A demonstration video of the system is shared by the authors in this link[1]. A comparison of three blockchain-based project for education were detailed – *Blockcerts, Sony Global Education (EGD) Blockchain, and OpenLearn Blockchain from Open University* – and can be seen in Table 2. Although these existing tools improves trust and reduce degree frauds, they still generate and issue credentials in a relatively black-box process. The authors platform aimed to extend these efforts by using smart contracts to automate and expose assessment procedures, facilitate the negotiation of personalized curricula, and generate credentials. Their conclusions suggests that the Blockchain University could increase trust in online educational providers, assessment procedures, education history and credentials.

Focusing on a different perspective, Garg et al [34]. proposed and developed an online reviewing system prototype - Blockchain-based Online Education Content Ranking System – communicating with a blockchain platform called Hyper Ledger Fabric. Generally, e-learning courses are evaluated with the help of their own review and rating mechanisms. These systems are usually centralized, storing valuable information at one location, therefore liable to manipulation, hacking, and tampering. The system provides a clear view to the learners to identify the course's quality offered by different online content providers using the federated rating. The federated rating is obtained by averaging the ratings provided by independent impaneled Subject Matter Experts (SME), endorsed by the stakeholders, and stored in a blockchain-based ledger to infuse trust amongst owners of different online learning platforms. This way, this helps simultaneously decrease disparity in

[1] https://www.youtube.com/watch?v=MP5jSItMenI (consulted in 20/03/2022)

the course contents made available by different vendors on the same topic and online education companies get a better view of the improvement needed to uplift the ranks and make it popular.

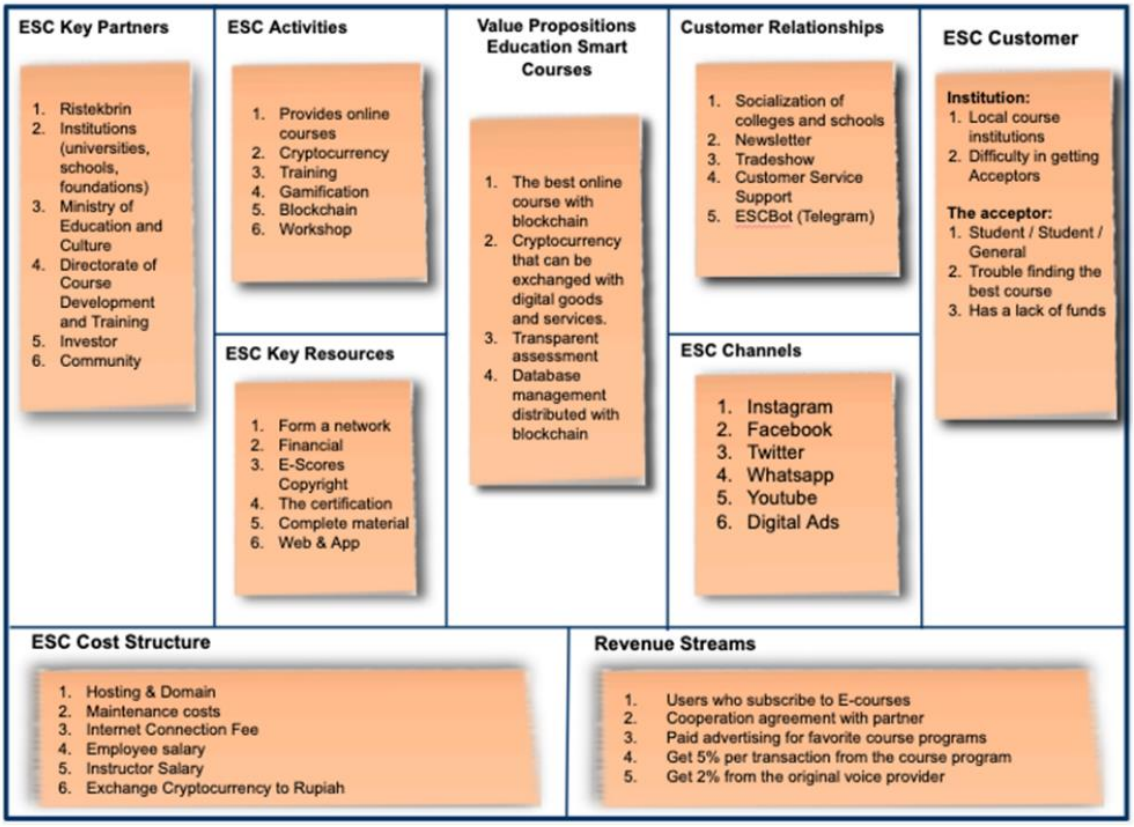

Figure 2 *- Business Model Canvas on ESC.*

Table 2 *– Comparison of existing projects: Blockcerts from MIT Media Lab, Sony Global Education Blockchain, and the OpenLearn Blockchain from Open University.*

Project (Based on)	**Features**
Blockcerts (Bitcoin)	Education providers can store a batch of certificates by paying for a bitcoin transaction, storing data in the OP RETURN transaction field on the global bitcoin blockchain.
Sony GED Blockchain (Hyperledger Fabric)	Developers at education institutions can use their application programming interface (API) to securely store learning history data and certificates, integrating with third-party e-learning systems.
OpenLearn Blockchain (Ethereum)	An experimental plugin for Moodle, a popular course management system, has been developed. Achievement badges can be stored on the Ethereum blockchain. Students can register for courses and receive badges in a "Student Learning Passport".

2.1.2. Challenges of Remote Assessment

From knowledge creation to evaluation of new acquired skills, academic integrity is in the midst of higher education institutions' value and reputation. The maintenance of the academic integrity at high standards stood always as a challenge and with the growth of the Internet, rising the access to databases and making the ready availability of information, this issue became even more problematic. Arkorful and Abaidoo [35], in their research work about the

effectiveness of using e-learning in teaching for HEIs, based on several studies, pointed out some advantages and disadvantages of this method. Regarding tests and assessments, the authors included it as a disadvantage and states that controlling or regulating cheating may be difficult, if not impossible. They also highlight problems upon piracy, plagiarism, and inappropriate use of copy and paste.

Mokdad and Aljunaidi [36], based on the disruption on the educational process in the various educational institutions led by Covid-19 pandemic and the surge of problems related to e-cheating and plagiarism that derived from it, performed research with 3 core questions: "1. Is cheating inherent in distance learning? 2. What kind of cheating is used in distance learning? 3. What are the measures taken to tackle this problem?". Authors concluded that for the first question, studies are still conflicting, without a clear perception if distance learning is better or worse than face-to-face learning. For the other two questions, the types of e-cheating used are many and varied, and two approaches were found useful to control plagiarism: preventive and therapeutic, with preventive approach having more effect in controlling plagiarism.

The research conducted by Kocdar et al. [37] aimed to study student's perceptions on cheating and plagiarism and trust in e-assessments according to their experience. Two public universities, one from Turkey and the other from Bulgaria, were chosen, comprising a total of 952 students. The cross-sectional survey consisted in a questionnaire of closed and open-ended questions and descriptive statistics, t-test [38], ANOVA [39] and thematic analyses were performed. The pool raised questions regarding student's feeling and perceptions toward e-assessment experience and the mode of learning they were involved in. Question with respect to concerns that might be an increase in cheating and plagiarism if face-to-face assessment were switched to online assessment was also raised. Results revealed that no significant difference was found on student's perceptions and feelings towards cheating and plagiarism prior to e-assessment experience. On the other hand, student's perceptions towards cheating and plagiarism regarding the mode of learning they were involved in showed significant difference. Another finding was that distance education students had lower trust in e-assessment than face-to-face courses, with 25.71% of them expressing a pessimistic view towards it.

Levine and Pazdernik [40] retrospective research yielded a four-prong anti-plagiarism programme and its impact on the incidence of plagiarism in a Post-Professional Doctor of Physical Therapy programme. Due to several factors regarding the students entering the program, such as the possibility of having an uncompleted university-level course, and receiving initial training in different countries, concerns arose from faculty. The research's result showed that a combination of structured education module related to education, the plagiarism detection software named Turnitin, implementation of policies and procedures, and support from institution's writing center, had significant

impact on mitigating these aspects. The plagiarism rate in the fifth year (0.35%) decreased to almost a third when compared to the first year (0.96%).

Nowadays, the application of blockchain technology to tackle the weaknesses in the assessment in the e-learning environment rose rapidly when looking for opportunities for solution. Li et al. [41] proposed a blockchain system for e-learning assessment and certification, which includes a new network structured based on the combination of public and private blockchains, as well as four smart contracts schemes for different purposes as follows: e-learning assessment and credit exchange; digital certificate issuance and secure storage; digital certificate verification; and e-learning voucher allocation. The system structured is composed of two types of user nodes, Learning Users and Education Authorities, and according to different node roles and the relationship among them, it was designed the network structure of the blockchain-based e-learning assessment and certification system, including three kinds of networks and two types of blockchains, as follows: Learning User Network (LUN), fully decentralized P2P network composed of all nodes of learning users; Education Certification Network (ECN), fully decentralized P2P network composed of all nodes of education authorities; Learning Assessment Local Network (LALN) and Learning Assessment Local Network of education authority X (LALN-X), in which each LALN is a local network dynamically constructed by one education authority in the system and LALN-X has the node of education authority X in the center node of the local network. The authors concluded that the proposed system has great potentiality in the future educational informatization application scenarios, such as unification of global e-learning assessment standards, creation of lifelong learning passports, as well as promotion of poverty alleviation in education.

More specifically to the programming field, Jing et al. [42] aiming to fulfill a gap on code plagiarism and code copyright protection, proposed a blockchain-based code copyright management system. The system was built upon three logical parts. First, an Abstract Syntax Tree-based code originality verification model is constructed, where the originality of the uploaded code is determined through its similarity to other original codes. Then, the P2P blockchain network is designed to store the copyright information of the original code, this way the nodes in the blockchain network can verify the originality of the code based on the code originality verification model. Finally, through the construction of blocks and legitimacy validation and linking of blocks, the blockchain-based code copyright management structure is built, making the whole process guarantee that the copyright information is traceable and will not be tampered with. According to the experiments, the accuracy and processing time of the system are shown to meet the code originality verification requirements, providing better response speed and storage efficiency.

2.2. CRYPTOGRAPHIC AND SIGNATURES

In order to later use of authenticity methods and to secure the information in the framework to be developed, some concepts of cryptographic hash functions and digital signatures must be introduced. Cryptographic hash functions are commonly used on blockchain technologies and digital signatures. Digital signatures and digital certificates are used for signing transactions and identifying the users under our framework. In the subsections ahead, a better look into these features is developed.

2.2.1. Cryptographic Hash Functions

There are plenty of cryptographic constructions for which one needs a function that is both easy to compute and hard to invert. Cryptographic hash functions fulfill this property. The hash function can be expressed as [43]:

$$Hash : (arbitrary\ size\ document) \rightarrow \{0,1\}^k \qquad (1)$$

A hash function (1) can be defined as the transformation of an input with an arbitrarily long document D that returns a short bit string H. It should possess three primarily properties. They are as follows [43]:

Linear time computation of Hash(D) should be fast and easy;

Exponential time inversion of Hash should be difficult. Given a Hash H, it should not be easy to find any document D in which Hash(D) = H;

Collision resistant it should be unfeasible to find any two documents D_1 and D_2 such that Hash(D_1) = Hash(D_2).

These functions help verifying the integrity of the data. A small change to a message should change the hash value in a way that a completely new hash value is created, totally uncorrelated with the old hash value. Figure 3 illustrates this.

There are many cryptographic hash algorithms. Some practical examples can be seen being used in Bitcoin, with SHA-256 [44], and in Ethereum, with Keccak-256 [45], blockchains.

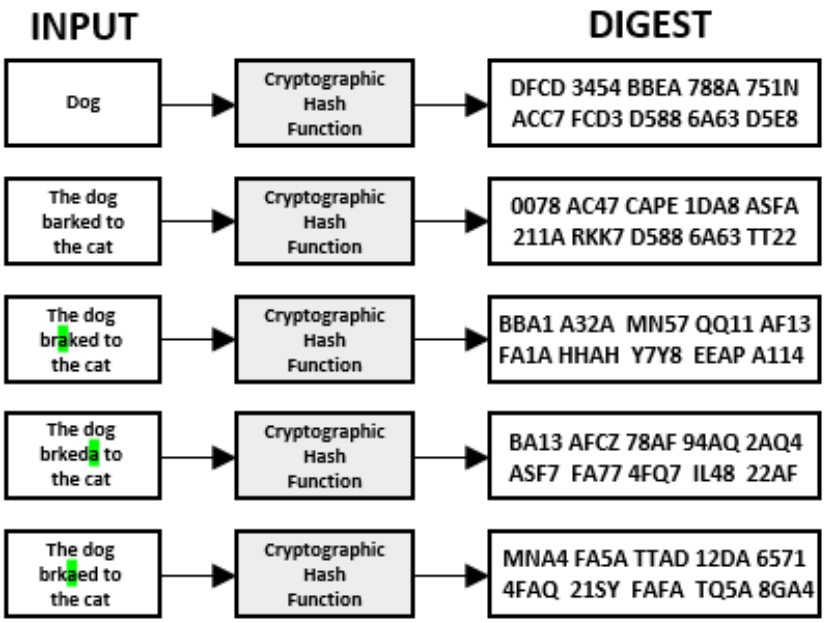

Figure 3 *- How a cryptographic hash function works.*

2.2.2. Digital Signatures

Digital signatures were made to solve a problem analogous to the purpose of a pen-and-ink signature on a physical document. Describing it in a more detailed manner, it is a mathematical scheme for validating the authenticity of digital messages or documents [46]. A digital signature scheme consists of three algorithms [43]:

Key generation algorithm it randomly selects a private key from a set of possible private keys and outputs the private and a correspondent public key;

Signing algorithm combines a digital document to be signed with a private key and produces a digital signature;

Verification algorithm it either accepts or rejects the message's authenticity based on the given message, the public key and the signature as inputs.

Figure 4 depicts the operation described above, where K^{Pri} is the private signing key, K^{Pub} is the public verification key, and D^{sig} is the digital signature.

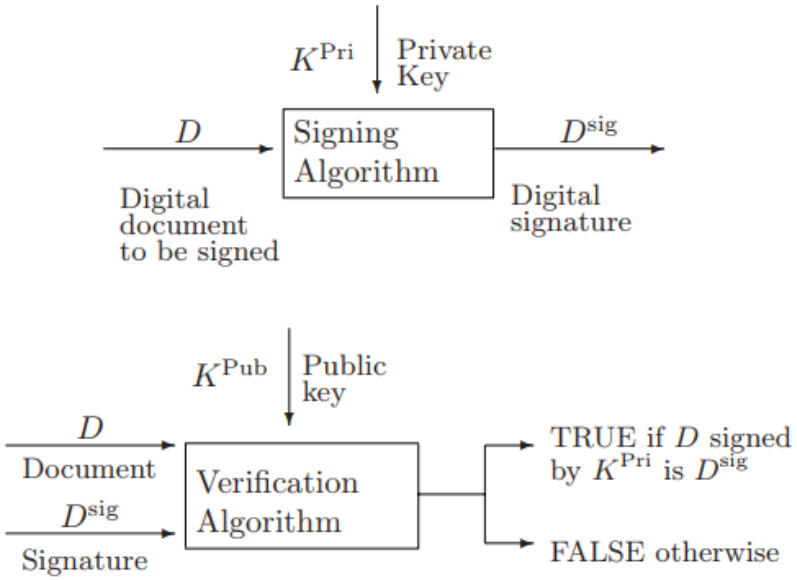

Figure 4 *- Components of a digital signature scheme [43].*

As the corporate world undoubtedly moves away from paper documents with ink signatures or authenticity stamps, digital signatures incorporate the role of adding assurances, identity, and acknowledgment of consent and approval by a signatory. The main reasons for its application can be summarized in three aspects:

Authenticity it allows to identify the messages' source;

Integrity a valid signature guarantees that any change in the message after the signature will make it invalid;

Nonrepudiation it prevents the signer of some information from denying having signed it at a later time.

One approach to guarantee these capabilities is the usage of a Public Key Infrastructure (PKI). PKI is a system of resources, polices, and services that support the use of public key cryptography to authenticate the partis involved in the transaction [47]. There is no single standard that defines the components of a public key infrastructure, but a public key infrastructure generally includes Certification Authorities (CAs) and Registration Authorities (RAs). CAs provides the following services: issuance of digital certificates; validation of digital certificates; revocation of digital certificates; and distribution of public keys. In Brazil, according to Provisional Act 2.200-2 [48], Brazilian law states that any digital document has legal validity if it is certified by ICP-Brasil (the official Brazilian PKI). On the other hand, in Portugal, the Drecree-Law 290-D/99 of August 2 [49] states that electronic signatures have the same evidentiary validity as handwritten signatures, as long as they are based on certificates issued by accredited certification entities. These certification entities can be public (National Security Authority) or private – *nowadays there are two private entities authorized, Multicert and DigitalSign*.

Regarding blockchain and digital signatures application, the Bitcoin example suits well to perceive their correlation. In order to transact on the blockchain, the user needs a wallet, or in other words, a program that enables the user to store and exchange bitcoins. This wallet is protected by a cryptographic method that uses a pair (private and public) of distinct but connected keys. When the user encrypts a transaction request with his wallet's private key, a digital signature is being generated to be used by blockchain computers to verify the source and authenticity of the transaction. This digital signature cannot be used for other transactions and if any character in the request message is tampered, the digital signature will also change. So, to send bitcoin the user needs to prove that he/she owns the private key of a wallet since he/she needs to encrypt the request message with it [50]. Figure 5 illustrates the description above.

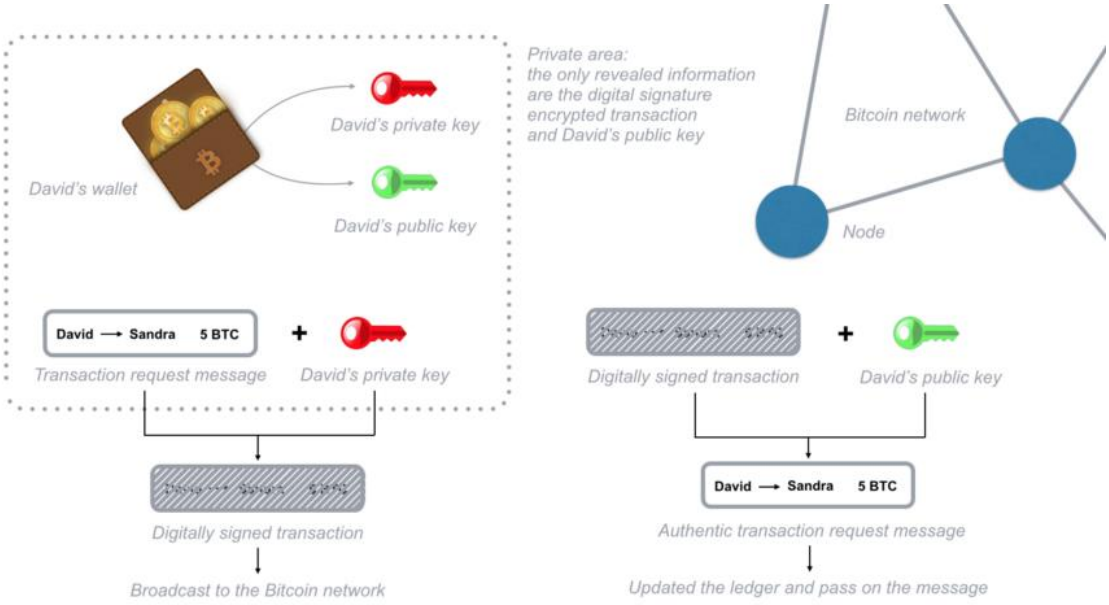

Figure 5 *- Digital signature transaction on a Bitcoin Blockchain [50].*

2.3. BASICS OF BLOCKCHAIN

This section covers the definitions and concepts of blockchain. It also addresses the various approaches of this technology on the educational sector, through advantages, applications and challenges to be overcome.

2.3.1. Blockchain Concept

Blockchain is a decentralized and immutable database – a chain of blocks (also called ledger) wherein information is stored, like transaction dates, timetable, quantities and/or members (members in the blockchain usually are not personally identifiable) [51]. Below, some other important concepts are highlighted:

Transactions. They are a set of data that is stored in each block. When a node receives a new transaction, it forwards it to the others nodes so

that the entire network carries the same content. After a new block is validated and included in the chain, the transactions in it become public and unalterable.

Block header (hash). It is a number that has the function of identifying the block within the chain. After all transactions have been validated and included in the block, the hash is generated. This data is included in the subsequent block to guarantee the chaining of the blocks.

Hash of previous block. In the header of each block is stored the identification hash of the previous block; this allows the successive chaining of the blocks. In this way, it is possible to go through the entire chain until reaching the genesis block, which in turn has the hash field of the previous block filled with zero because there are no previous blocks.

Nonce. It consists of a variable used to change the result generated by the header. It is used to prove that a block has been validated and it meets the criteria established by the network.

Block height. The blocks are included in the chain sequentially. The difference between the position of a block and the genesis block of the chain is called block height.

Timestamp. Next to each block is stored the moment it was generated. This record is given by a number that represents the exact date and time of its creation.

2.3.2. Types of Blockchain

The blockchain system can be configured in three different ways. Each one has its own specific configuration and vary accordingly to the needs of the project. Following, these configurations are described [52].

Public. Allows anyone to participate in and contribute to the network. In this way, public blockchains are valuable because they provide a truly decentralized, democratized, and authority-free operation.

Permissioned. Unlike public, it only allows verified participants, such as members of an organization, who are invited and validated before joining the network.

Private. Similar to permissioned, with the difference that private is maintained and owned by a single organization.

2.3.3. Types of Mining Protocols

Although blockchain may look like a homogeneous technology, there are some variations to its network function, especially on the type of consensus mechanism that each blockchain uses. A consensus mechanism is the process employed to reach an agreement about the information in the distributed network (e.g., legitimacy of transaction, order of occurrence) [53]. Here, we

take a look at the main blockchain consensus mechanisms for better understanding:

Proof of Work (PoW). Most popularized by Bitcoin; miners operate computing hardware to run network nodes that employ computing power to algorithmically solve mathematical puzzles called proofs of work. The miner that solves the puzzle first confirms the most recent transaction block on the blockchain. The successful miner then transmits the new block to all other nodes, which in turn confirm its accuracy and add that block to their copy of the blockchain, building a verifiable record of data for the entire network. This verification process represents a consensus. Only when this data is confirmed can a new block be added to the network.

Proof of Stake (PoS). PoS is the second most popular consensus mechanism and solves many of the disadvantages found in PoW blockchains, such as lack of speed, poor scalability, inefficient energy consumption, and higher barrier to entry. Instead of miners validating transactions, PoS blockchains simply have validators. Validators are network node operators, that validate data, similar to PoW systems, but there is no energy-intensive computational process to earn the right to validate. Instead of working to solve proof of work, validators "bet" some of the native tokens of the blockchain to become eligible for selection as a validator node. The potential validator will essentially wager native cryptographic tokens from the blockchain to serve as a warranty. When the time comes to validate the data held in the transaction block in a PoS blockchain, the system randomly selects a validator to confirm the data. Although random to some extent, certain variables can make it more likely that a validator will be chosen, including the number of tokens a validator has staked. When the block is confirmed, that validator is typically rewarded with network transaction fees, and the process begins with a new block.

Private and Consortium. The types of blockchains that use PoW and PoS consensus mechanisms are typically public and decentralized. However, there are other categories of blockchains – consortium blockchain and private blockchain. A private blockchain is a blockchain controlled by a centralized entity that determines who can interact with the blockchain, verify transactions, and who can view the information recorded to the blockchain. A consortium blockchain is a distributed ledger controlled by multiple entities, each of which operates a network node, participates in the consensus, and has permissions to view certain types of data. Given the lack of decentralization in these networks, this type of blockchain technology is often referred to as Distributed Ledger Technology.

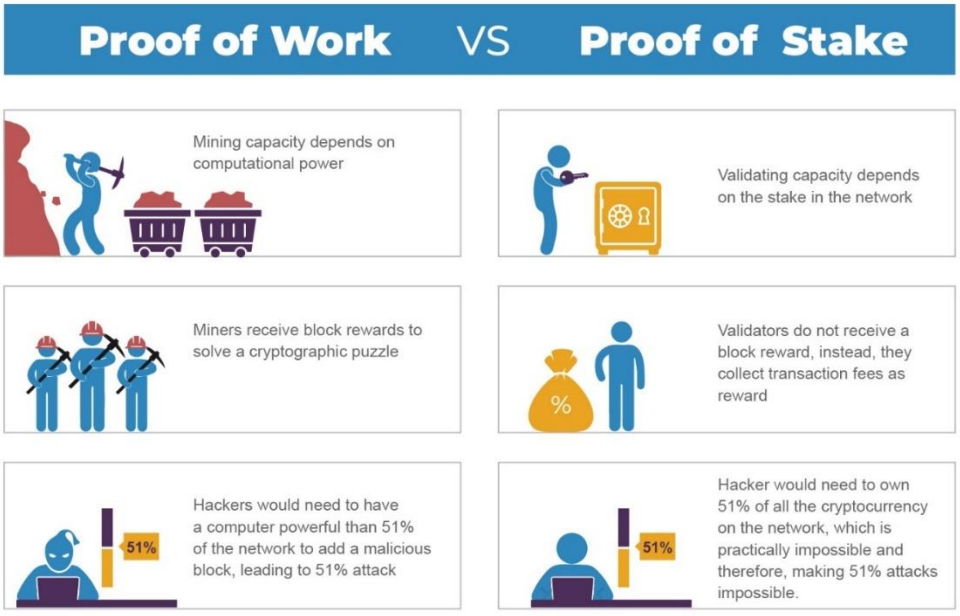

Figure 6 *- Proof of Work vs. Proof of Stake [54].*

2.3.4. Smart Contract Concept

It is a computer program on the blockchain, which contains the terms of the agreements between two or more peers, and can be executed in an automatically and safe way [20]. The smart contracts receive as input a series of conditions that remain constantly monitored and when they are met, the contract executes itself. The whole process is automated and can be totally virtual or mixed, as a complement to paper-based contracts. Hence, the smart contract strengthens and facilitates the negotiation and performance of a contract. They are divided in three steps [51]:

Step 1. Codification

Initially, the contract is coded in a programming language. In the code, instructions that the contract must execute are carefully defined and must be in accordance with the interest of the parties.

Step 2. Submission to the blockchain

After encoding, the code is encrypted and sent to other computers via blockchain. This occurs in a similar way to cryptocurrencies transactions.

Step 3. Execution

The blockchain receives the code and processes it on one of its nodes. The network then updates the registries so that all nodes contain the results of the contract processing. The contract is then monitored by the network.

2.4. EVOLUTION OF THE BLOCKCHAIN TECHNOLOGY

Even though the blockchain technology got to the spotlight in 2008, with the publication of a white paper from Satoshi Nakamoto enlightening its concepts and Bitcoin [55], its roots came from a combination of some important technologies previous to the date abovementioned.

2.4.1. Early Technologies (1979 – 2007)

In his 1979 Ph.D. thesis for Stanford University, Ralph Merkle introduced an approach to public key distribution and digital signatures called tree authentication, also known as the Merkle Tree. Later on, the idea was patented as a method for providing digital signatures, with a data structure for verifying individual records [56].

In 1982, David Chaum in his dissertation for the University of California, Berkeley, named "Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups", described a public record-keeping system that protects individual privacy through physical security. Many of the elements of blockchains are expressed in his work ([57], [58]).

Stuart Haber and W. Scott Stornetta, in their article published in 1991, proposed a solution what many people have come to know as blockchain [59]. It was presented a solution for preventing users from tampering timestamps of electronic documents. The outmost goal was to maintain the privacy of the document itself without the need of a timestamping service for record-keeping. A year later, in 1992, the authors upgraded their design to incorporate Merkle trees, which enabled the collection of more documents on a single block [60].

Other concepts such as peer-to-peer (P2P) network and proof-of-work (PoW) also contributed to build the blockchain foundation. In 1999, the concept of P2P network was popularized by a company called Napster. Their service made it possible to build a system that could benefit from a gigantic net of computers' computational power and storage. Some may still argue that Napster used a centralized server and was not a pure P2P network, but it definitely gave and push into P2P network development [61]. In 1997, Adam Back introduced Hashcash, a mechanism to throttle systematic abuse of un-metered internet resources such as email, and anonymous remailers [62]. In 2002, Back published a new article introducing a PoW algorithm that provided a denial-of-service counter-measure [63]. Then, in 2004, Hal Finney invented the Reusable Proof-of-Work (RPOW) as a prototype for a digital cash. It was a mechanism for receiving non-exchangeable hashcash token in return for an RSA-signed token. RPOW is considered a significant early step in the history of digital currency and a precursor to Bitcoin [64].

2.4.2. Bitcoin and its Unfoldings (2008 – 2015)

In 2008, Bitcoin came as the first application of blockchain technology. Satoshi Nakamoto detailed it in his white paper as an electronic peer-to-peer cash system [65]. According to his paper, blockchain infrastructure would support P2P transactions without the need of a third party to mediate. The concepts and technologies from the previous decades formed the Bitcoin architecture. The concept of "chain of blocks" is also introduced in Nakamoto's paper. Actually, the definition given for electronic coin was a chain of digital signatures. This would be done by digitally signing a hash to a previous transaction and the public key of the next owner and adding theses to the end of the coin.

Ever since its launch, Bitcoin rose immensely in its popularity and market value. Eventually, this brought attention to blockchain applications and the principles and capabilities of the digital distributed ledger. Despite the setbacks with Bitcoin experiences, such as the Silk Road [66] and others, many other innovations in the area started to grow. One innovation that worth standing was the creation of the Ethereum Foundation, launched in 2014, based on a 2013 white paper by Vitalik Buterin [67]. Buterin differentiated Ethereum from Bitcoin Blockchain through a new feature that would allow people to record assets other than currency, expanding it from being a cryptocurrency to being a platform for developing decentralized applications. In 2015 the Ethereum Blockchain was officially launched [68], and from then on it grew to become one of the biggest applications of blockchain technology. An important feature that supports this allegation is its ability to use smart contracts to perform different functions. The Ethereum blockchain community plays also an important role to its success, gathering an active developer network.

2.4.3. Blockchain and Market Adoption (2016 – present)

With the foundations laid by the previous versions, Blockchain nowadays describes solutions and approaches that make blockchain technology usable to business demands. The benefits to business can be many, such as improving transaction's security, managing digital relationships, eliminating intermediaries, and tracking and tracing products with supply chain and ERP integration. Industries ranging from financial services, healthcare to retail are some to mention that are benefiting from these aspects. PwC's global blockchain survey in 2018 illustrated the industries that were taking lead in blockchain adoption, as seen below [69]:

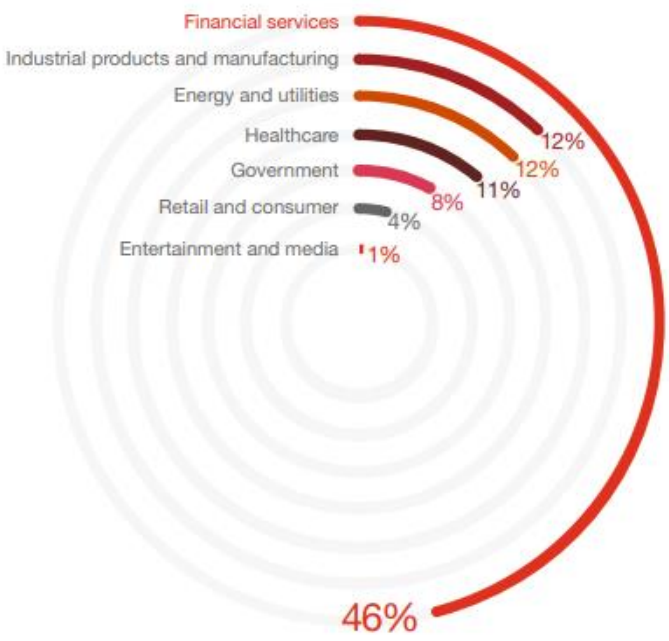

***Figure 7** - Industries seen as leaders in blockchain [69].*

Financial services lead the initiatives on blockchain application as expected. But, for other areas, its applicability maybe not easily understood. So, some of these new areas of blockchain application and its benefits are better detailed as follows ([70], [71]).

Healthcare. Patient's data such as age, gender, and basic medical history data like immunization or data signs are all eligible for blockchain recording. None of this information could help identify any particular patient, so it could be shared and accessed by numerous individuals without violating any privacy concerns. These data, collected by medical devices, could be stored on a healthcare blockchain and append it to personal medical records. A key issue currently facing connected medical devices is the isolation of the data generated, but the blockchain could be solution for this.

Supply Chain Management. Blockchain provides a new dynamic means of organizing tracking data and putting it to use. Its immutable ledger makes it perfect to perform tasks such as real-time tracking of goods as they move from depart to destination. Therefore, no unauthorized person can change, manipulate, or erase the data.

Media. Eliminate fraud, reduce costs, and protect Intellectual Property rights of content are some of the usability of blockchain in this sector. By eliminating intermediaries, the exchange of the content among developers, publishers, and end-users at a reasonable cost can be streamlined.

Gaming. Gamers can collaborate and make secure transactions using blockchain. They can start generating revenue by reselling their in-game amenities to other players. The gaming market in 2021 reached $175.8Bn in

revenue [71], and this in-game services/components are gaining attention more than ever.

Energy. Energy supply transactions, providing the bases for metering, billing, and clearing processes, are all usable ways for blockchain in the energy sector according to PwC [72]. Other potential applications include documenting ownership, asset management, emission allowances, and renewable energy certificates.

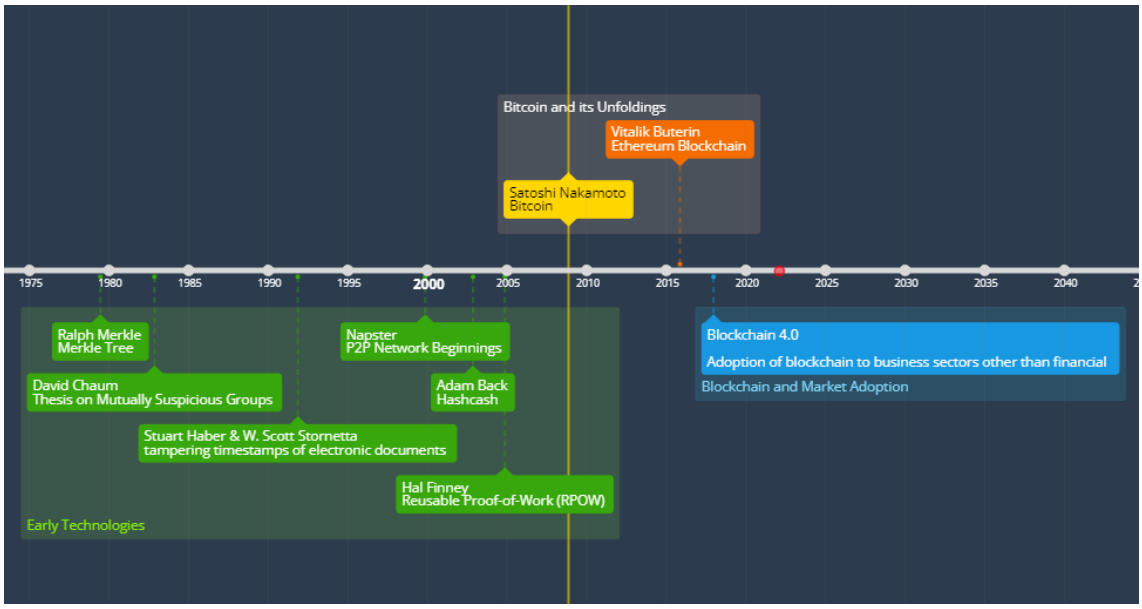

Figure 8 *- Blockchain Timeline.*

2.5. BLOCKCHAIN IN EDUCATION

The blockchain technology is already far beyond its initial stage, when it was aimed at enabling the operation of the cryptocurrencies, more specifically Bitcoin. With the years going by, and the benefits of the technology being redirected to others areas, such as other aspects of financial services and throughout healthcare, utilities, contracts, and public sector, for example [73]. The educational sector is one of the newest participants in this transformation and there are some key dimensions in the process of teaching and learning that can be improved [74].

First, is the empowerment for learners, also called self-sovereignty. Through blockchain, the data is associated with the student's identity is not controlled by a central administrator, such as a university, but by the student. Then, there is the enhancement in security and efficiency for educational institutions, business and students. Thanks to the immutability of the blockchain, students will not be able to change educational certifications obtained in the past that are stored on the blockchain, while this can easily be

done with paper records. Lastly, there is the integration of trust and transparency. Because blockchain ensures that students will not be able to change their grades, diplomas, and certifications, it gives employers the assurance that the job applicant actually has the skill needed to succeed in the workplace.

2.5.1. Application of Blockchain in Education

According to Steiu [74] analysis to different researchers and entrepreneur's work, there are two major applications of blockchain: certificates and identity management and enhancing and motivating lifelong learning. Morais et al. [51] goes further on its analysis of different research works, and beyond both topics previously mentioned it also points out the usability of smart contract by educational institutes for tuition payments and student loan; the use of blockchain to guarantee the authenticity, integrity and immutability of academic documents; automatic verification of credits and title certificates; and registering knowledge in blockchain. These topics and some works related are described below.

2.5.1.1. Digital Certificate and Diploma Management

One of the main discussions about the usefulness of Blockchain for education falls on registration of diplomas. The diploma is considered one of the most important documents issued by educational institutions, as it serves as a document that proves the training received by the student and gives him the necessary authorization to exercise his profession [75]. However, there are several cases of not only diploma, but also resumes forgery. This can compromise the credibility of educational institutions and make it difficult for the companies to assess the competencies of candidates. According to Grolleau et al. [76], roughly 25-30% of all resumes contain some falsehood about qualifications, and there were more than 2 million fake degrees sold in the United States alone.

Founded in 2018, with a mission of building a trusted infrastructure for academic digital credentials, the Digital Credential Consortium is considered a key academic initiative, building a global infrastructure and leading through partnerships among top universities around the world [77]. One of the main educational institutions ahead of this consortium is MIT. Together, MIT Media Lab and Learning Machine collaborated to develop BlockCerts, an open standard for issuing and verifying credentials on a blockchain ([78], [79]). The goal is to give ownership of the official records to the beneficiary, breaking the dependency on issuing institutions for verifying their own credentials and achievements.

Another example of educational institution's offering on certificate and management blockchain applications by educational institutions comprises University of Nicosia, with accredited courses through verifiable certificates with blockchain ([80], [81]).

A similar proposal is presented by Huynh et al. [82], where the possibility of using blockchain for issuance and validation of digital certificates to ensure security and prevent tampering. The authors propose the creation of UniCert, an application that will receive the certified data, make its registry in a local PostgreSQL database and send a hash of the document to the network nodes of the blockchain. This way, the level of safety is higher since the registry is done on multiple levels – local database and blockchain – making it even harder for possible attacks to the data.

Aside from academic implementations, there are also several private companies developing solutions based on blockchain for learning certification purposes. BCDiploma, for example, is a European start-up which created its decentralized service based on Ethereum token, the Blockchain Certified Data Token (BCDT), utilizing a patented one-click technology for accessing certified compliant data [83]. Hence, students can use their generated URL link containing their academic documents (diplomas, certifications, transcripts or skills) and employers or third parties can access and verify the certificate with a single click [84].

2.5.1.2. Enhance and Motivate Lifelong Learning

Nowadays, personal and professional development breaks the barrier of conventional education. Certificates plays an important role on the individual learning records, becoming essential for their professional careers. Therefore, having these records stored in long-term available and tamper-proof ledgers become of utmost importance [85].

Liu et al. [86] proposes the use of blockchain to record student-generated information by creating a distributed platform, based on the Hyperledger Fabric, that will bring transparency, security, and integrity to the data. The prototype system serves to register different information related to each student, such as their grades, school history, activities developed, among others. This information is not limited to one institution, but also from all other places where the student has been.

In parallel, Zhong et al. [87] introduces a platform that serves to register students and store their academic/school activities' information and utilize a mechanism to reward students, in cryptocurrencies, for their achievements. Later, these coins can be used to purchase some paid or encrypted files, which can avoid plagiarism and protect intellectual property. The platform is developed on NodeJs and record the data in a MongoDB database, which are sent to the blockchain.

In this context, manifold companies are undertaking on this out-of-classroom education, such as lifelong learning development, aiming to enhance the learning process. BitDegree [88] and ODEM [89] stands out in this area. The first is a platform that gamifies online education and rewards users with tokenized scholarships for completing courses or reaching milestones. The

latest, students interact with academic professionals, using ODEM token, who offer personalized learning experiences. ODEM Network connects all parties (students/professionals, employers, educators, and educational organizations) to create in different subnetworks (Trust, Employment, Marketplace) a complete atmosphere of trustful connections, making learning, teaching, and employing more engaging and effective by using blockchain.

2.5.1.3. Using Smart Contracts in Academic Environments

The benefit of executing a code that runs on top of a blockchain to sign an agreement between untrusted parties without the interference of a middle man in the academic environment have been explored in different manners.

Ocheja et al. [90] proposes an application that gets access to the students database, gather their main information – such as grades, evaluations and behavioral data – and arranges in the form of smart contracts. These contracts will be executed as the student progresses throughout the course, thus ensuring that all their activities in the blockchain are recorded. This way, it allows a bigger interoperability between the educational database and will guarantee the immutable record of the data.

Another way smart contracts are being explored is for payments. Rooksby et al. [91] bring the creation of a Ethereum based blockchain platform for the university environment. Students receives a cryptocurrency called Kelvin Coin as reward through good performance in academic activities. Then, with the coins, students can pay for new courses.

Yet another different approach was made by Gilda et al. [92] in the context of utilizing smart contracts to record consent information. They propose a smart contract solution for STEM Education's process of approval to be implemented on blockchain. This would provide several benefits such as: immutable ledger of how data has been approved, by whom, and for whom, with easy access; parental control over revocation of access in the event of unenrollment or misuse of data by third parties; and high level of security for student data access outside of the system.

2.5.1.4. Use of Blockchain to Guarantee the Authenticity, Integrity and Immutability of Academic Documents

In addition to diplomas and certificates, there are several other academic documents (e.g., assessments, academic history, etc.) that serve as proof of education received by the student and need to be issued and stored in a securely way. Currently most academic documents are printed on paper and stored in physical files and the existing digital databases are mostly centralized and of restrict access. Without mentioning the extra cost of double storage, the exchangeability of information between institutions becomes a harshly job for the students when transferring to a different school [51].

On their paper, Turkanovic et al. [93] propose a global higher education credit platform called EduCTX. Based on the concept of the European Credit Transfer and Accumulation System (ECTS), the blockchain platform aims to avoid language and administrative barriers when recognizing students' academic training. On the platform, each university stands as one node in the blockchain, and stores a copy of the database. This way, information remains continuously available for consulting by students, employers and other educational institutions by using an access key that works as an identifier.

2.5.1.5. Blockchain Applied to Distance Assessment in HEIs

As it could be seen in the previous topics, a variety of blockchain applications in the educational sector are being developed and applied. Currently, most of this effort is being directed to digital certification management and digital wallets for academic achievements. Therefore, a deeper look was made in order to identify projects that approaches the main goal of this actual paper, which is building a framework that could mitigate or eliminate the use of plagiarism or e-cheating in assessments in the HEIs. Several papers were analyzed using different keywords for the search, such as "blockchain", "framework", "e-cheating", "HEI", "assessment", "academic dishonesty". A few projects with slightly similarity to the topic were found. To mention, Li et al. [41] with a full blockchain system for e-learning assessment and certification composed by the combination of public and private blockchains, as well as four smart contracts schemes for different purposes, being one of these smart contracts aimed to e-learning assessment and credit exchange. And Jing et al. [42], with a blockchain-based code copyright management system composed by three parts, a code originality verification model, a P2P network to store the copyright information, and a chain of blocks to guarantee that the information will be traceable and will not be tampered. Beyond these two, no other paper was found regarding the creation of a blockchain framework with the specific purpose of mitigating e-cheating or plagiarism in online assessments. Thus, despite not having a big research development on this specific topic, this brings with itself the need for new works to be conducted in order to tackle this sensitive and important subject.

2.5.1.6. Summary of Blockchain Applications in Education

Overall, a handful of studies and projects were presented covering different undertakings regarding the usage of blockchain technology in the educational sector, more specific the HEIs. A total of 12 projects were analyzed, in which eight can be classified into a record-keeper blockchain initiative. One was related to the efficiency of financial and academic progress. Three refers to the privacy and security of the data. When taking into account whether the project is more targeted to the student or more to the institution, five out of 12 were detected as only student focused, while 3 were only institution focused. Four other projects were identified as following both approaches, student and institution focused. When we dive into the record-keeping projects, it is

possible to notice that projects related to diploma and certificates management tend to be more student oriented, while lifelong learning encompasses both student and institution. Table 3 displays the projects analyzed by its characteristics.

Likewise, another table was created, Table 4, in order to identify what kind of requirements, techniques, and methods were used in each related work described in the previous sections.

Table 3 *- Use cases of blockchain in the educational sector.*

PROJECT	AUTHOR	SF	IF	DOMAIN
Open standard application for issuing and verifying credentials on a blockchain (Blockcerts)	MIT Media Lab & Learning Machine [78,79]	X		RK
Accredited courses through verifiable certificates with blockchain	University of Nicosia [80,81]	X		RK
Issuance and validation of digital certificates	UniCert [82]	X	X	RK
Decentralized service based on Ethereum token, with one-click technology for accessing certified compliant data	BCDiploma [83,84]	X	X	RK
Distributed platform based on the Hyperledger Fabric to record stundent-generated information	Liu et al. [86]	X	X	RK
Platform to store academic activities' information and reward students with cryptocurrencies for their achievements	Zhong et al. [87]		X	RK
Gamification of online education with tokenized rewards for milestones completion	BitDegree [88]		X	RK
Blockchain-based network for interation between parties to create an atmosphere of trustful connections	ODEM [89]	X	X	RK
Utilization of smart contracts to follow student's progress to guarantee immutability of the data	Ocheja et al. [90]	X		PS
Ethereum blockchain platform that rewards students with cryptocurrency, via smart contracts, which can be converted for paying new courses enrollments	Rooksby et al. [91]	X		FE
Smart contract solution for STEM Education's process approval	Gilda et al. [92]	X		PS
Global higher educational credit platform based on the ECTS concept (EduCTX)	Turkanovic et al. [93]		X	PS

SF - Student Focused, IF - Institution Focused
RK - Record-keeping, PS - Privacy and Security, FE - Financial efficiency

Table 4 *- Comparison of related work by its requirements, techniques, and methods.*

RELATED WORK	Public Blockchain	Permissioned Blockchain	Uses its own cryptocurrency	Privacy concerns	Process automation	Smart Contract	Credis stored as transactions	Degree certificates stored as transactions	Verification mechanisms	Revocation mechanisms
MIT Media Lab & Learning Machine [78,79] (2019)	X							X	X	X
University of Nicosia [80,81] (2017)	X							X	X	
UniCert [82] (2018)		X						X	X	
BCDiploma [83,84] (2018)	X							X	X	
Liu et al. [86] (2018)		X				X	X	X		
Zhong et al. [87] (2018)	X		X			X	X			
BitDegree [88] (2017)	X		X			X	X	X		
ODEM [89] (2017)	X		X			X		X	X	X
Ocheja et al. [90] (2018)	X			X		X	X		X	
Rooksby et al. [91] (2019)	X		X		X	X	X	X		
Gilda et al. [92] (2018)		X		X		X			X	X
Turkanovic et al. [93] (2018)		X		X	X		X			

3. THE PROTOTYPE DESCRIPTION

This section presents a blockchain-based framework solution to enhance the authenticity and integrity of the remote assessment process in a HEI. Lecturers and students share and access assessments through a combination of private and public keys. After the completion of each assessment, the submission is digitally signed, timestamped and recorded on the blockchain. Following, our proposal is introduced.

3.1. THE PROTOTYPE STAKEHOLDERS

Our solution involves three types of stakeholders: HEI, Professors, and Students. The first type is the Higher Educational Institution (HEI), which is responsible for evaluating and approving the types of assessments that are going to be proposed in the classes by the designated Professor. A second role is to store the Student's information that are relevant to the institution so they can be properly identified and be incorporated in the system (e.g.: public key, suitability to enroll in class, etc.). In a nutshell, the HEI acts as a central entity in the access rights and validation process. Moreover, HEI is the node responsible for deploying the smart contracts in the blockchain network. These smart contracts will make the interface between the participants and the blockchain. The Academic Director of each faculty, or its direct associate, can serve as the figure responsible for this node.

The second type are the Professors. They provide all the assessments that the Students are supposed to complete to fulfill all demands in order to be approved in the subject. They are also responsible for registering the students in the class and for issuing the conclusion certificate of the subject. When a student completes an assignment, the Professor records his or her progress in the blockchain. This way, students attend classes and fulfill the assignments to be approved in the class.

The latest, Students, is responsible for completing each assessment provided in the class and be awarded a conclusion certificate once they complete all the tasks demanded. There are different types of events in each step of the solution. All events are recorded in the blockchain despite their type. If a student completes an assessment, an event is recorded. If a student completes the course, this becomes an especial event because it requires to be checked if all assessments were completed with a minimum passing grade in order to grant this student a certificate of completion of that subject. This checking is done automatically by a smart contract.

Besides the external participants, the blockchain network and the smart contracts also plays a part in the interactions of the system. The blockchain works as a decentralized database for the student's progress in their pursuit of an academic diploma. To interact with the network, each participant needs an account generated from his or her public key. This way, the characteristics such

as authenticity, integrity and nonrepudiation are incorporated to the system to mitigate attempts of misconduct during the online assessments. Smart contracts, on the other hand, make the interface between stakeholders and the blockchain network, automating the processes in a transparent and auditable way. Another responsibility is to manage the access rights in order to update data in the blockchain.

Figure 9 summarizes all the interactions described above between participants and smart contracts. It all starts with HEI on the upper left corner deploying the first smart contract, and then it follows the direction of the arrows through a continuous flow.

It worth noting that this arrangement can be altered or extended with ease in case of need. For the system to work, these three participants can accomplish all task needed, but other figures can be inserted to segment the tasks or add new functionalities.

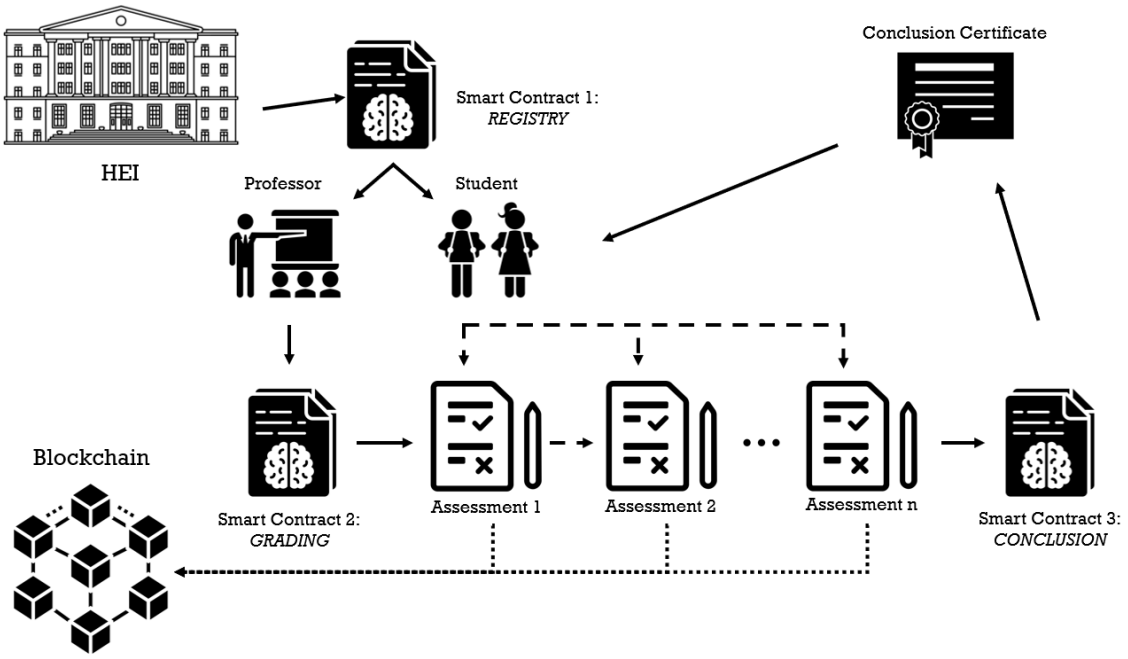

***Figure 9** – Stakeholders' interaction in the system.*

3.2. THE FRAMEWORK COMPOSITION

In this topic, the framework will be presented in more depth. Beyond the stakeholders introduced in the previous section, to automate the process, three smart contracts are implemented in the blockchain. Their principles are detailed below.

The first smart contract, called REGISTRY, guarantees the authenticity of the Professor and that it can only record events regarding the students enrolled in their classes. To correctly identify the Professor, REGISTRY records the Professor's credentials in the blockchain (public key). This way, all transactions made by the Professors must be paired with their private key. The second smart

contract is called GRADING. Each occurrence of this smart contract has to do with a class and lists the students, identified by their address in the blockchain, that are enrolled in it and the assessments they need to complete. GRADING allows a Professor to update the student's progress in the class in order to list the assessments he/she has already fulfilled. The third smart contract, called CONCLUSION, is responsible for issuing a completion certificate after GRADING indicates that all assessments were pursued. Figure 10 illustrates the solution's workflow involving the stakeholders and the smart contracts.

The framework's process begins with HEI deploying a smart contract named REGISTRY. This smart contract works as an identity manager. It receives as inputs both Professor's and Student's Ethereum account addresses. It also has functionalities to manage these accounts, such as to update or revoke them. Since HEI is responsible for regulating which Professor and which Student should be part of the system, these functions are exclusively HEI's responsibility for deployment. HEI here is represented as one institutional part of the actual HEI, which is responsible for the subject in matter. So, the personal figure to be in charge of these deployments could be an academic director, or maybe a section manager of the corresponding department.

Next, HEI and Professors works together to define what are going to be the assessments for each professor's subject in particular. For example, how many assessments will be necessary to fulfil the semester and their types (e.g., multiple choice evaluation, research presentation, quizzes, etc.). Thenceforth, HEI initiate multiple instances of the smart contract GRADING. Each instance represents a discipline to be taught in the semester associated with the corresponding Professor responsible for lecturing that particular discipline. This smart contract will work as the interface between the Professor and the blockchain. Moreover, it has functions to register assessments and students, and to update the student's progress through the discipline. Analogous to REGISTRY, only the designated Professor can give commands to GRADING after deployment. It is important to highlight that every execution of GRADING needs to be checked trough REGISTRY. This is done in order to check if the Professor's credential is still valid or was revoked by the HEI for some reason. If it was revoked, no state changes will be allowed and the process ends. Otherwise, the Professor can record the assessments the students need to complete to receive a passing certificate on that particularly discipline. Since the goal of the project is to mitigate any kind of plagiarism or e-cheating during online assessments, digital signature was included in the next step. The reason for that is to profit from the important aspects that this tool provides, such as authenticity, integrity and nonrepudiation. Thus, when the Professor inputs assignments on the blockchain, he or she digitally signs it with the Student's public key and his or her private key. This way, only the specific student can open his or her assignment using his or her own private key and the Professor's public key. In this process, we can raise the degree of confidence in relation to whom is taking that assignment (authenticity). We can also guarantee that after submitting his or her assignment, it cannot be tampered since that a

slightly change in the content would create a totally different output hash (integrity). Lastly, it safeguards the Professor or the institution from a not so well intended Student trying to deny one of his or her assignment already submitted (nonrepudiation).

Another step taken towards the goal of reducing plagiarism on the assessments submitted to the system is the integration of plagiarism detection tools in the process. Before registering the assessment's conclusion on the blockchain, the Professor should run the assignments through an external anti-plagiarism tool (e.g., Turnitin, Plagium, or other similar) for validation. This step is represented in the framework's flowchart because of its extremely important part in the process. However, on the actual framework developed for this dissertation, this step was skipped. More explanation about this is noted in Section 7, devoted to future work implementations.

The following steps take care of the progression of GRADING in the network. For each assessment a Professor offers, it provides the identification of the students to the corresponding instance of GRADING. As the time goes by, and assessments are accomplished during the semester, Professor use GRADING functions to update student's status. When GRADING spots the completion of all assessments by a Student, it creates a new instance of a smart contract called CONCLUSION. An event is registered by CONCLUSION stating that the Student has finished his or her discipline and is granted a certificate of conclusion in the blockchain. Receiving a conclusion certification does not directly mean that the Student have finished with a passing grade and is apt for the next discipline in the academic curriculum. There is a field indicating his or her final grade. This function could be treated by a different system and is not part of this project scope.

All in all, this project contemplates essential properties that complies with our initial proposition's goals. Since all transactions are recorded in the blockchain, the information shared are tamper-proof and cannot be lost (integrity); it uses digital signatures to access sensitive information, such as the assessments (authenticity); anyone with the given permission can check the information and inquire in respect to the process of evaluation and the validity of the information (transparency); lastly, it includes in the process only the necessary individuals. After all arrangements are set up, it becomes automated by smart contracts, mitigating flaws and paper-based processes (reliability).

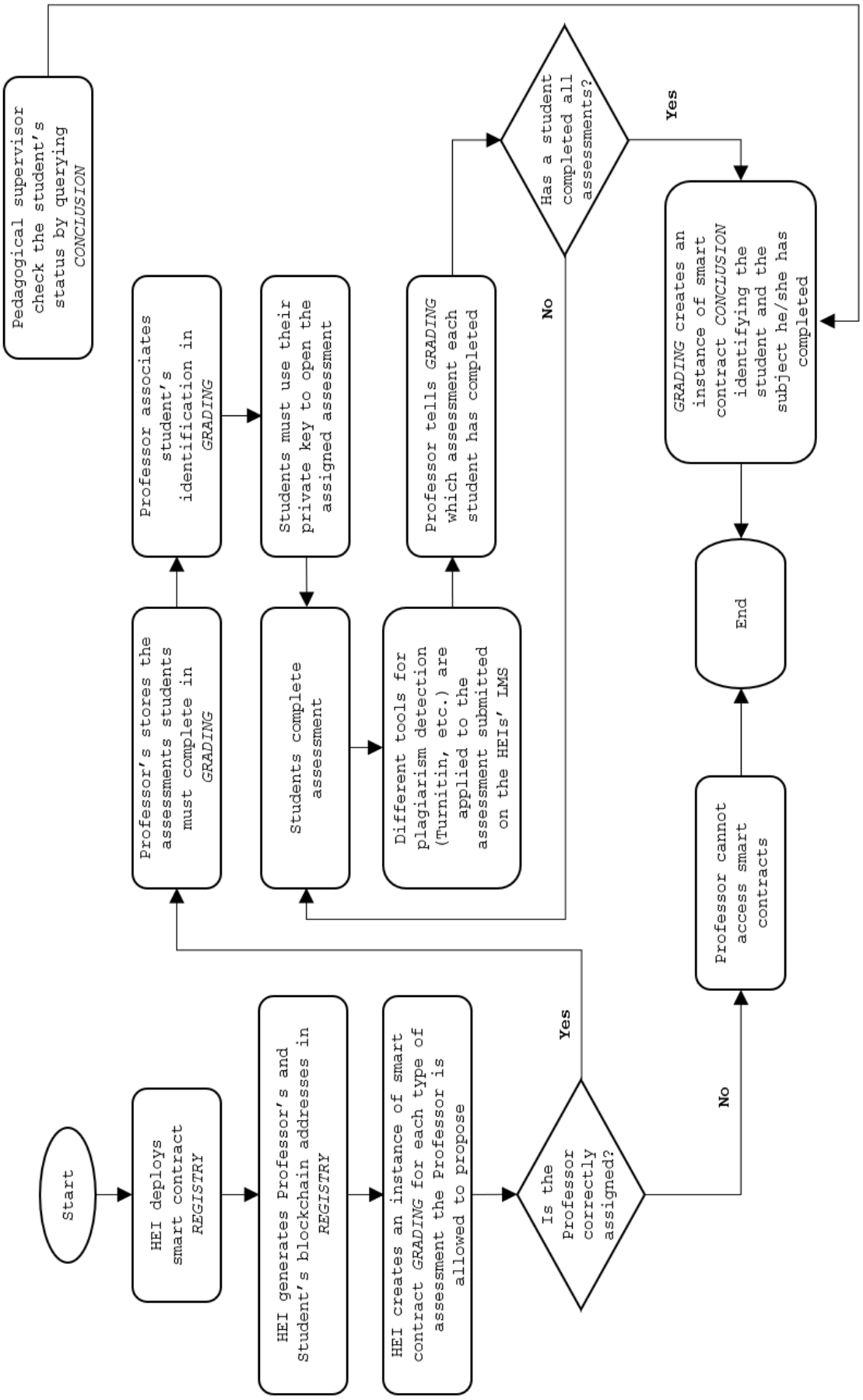

Figure 10 *- The flowchart of the framework's logical process of functioning.*

4. THE PROTOTYPE IMPLEMENTATION

This section describes the development of each smart contract and the testing results of the system in a controlled scenario. The programming language used for developing the smart contracts was the object-oriented Solidity [94]. We also used an online Integrated Development Environment (IDE) named Remix [95] to simulate the deployment of the smart contracts in the Ethereum Blockchain network. Figure 11 illustrates the class diagram of the smart contracts.

The Ethereum blockchain was chosen for this project for three main reasons: credibility of the network; material availability for support; and cost and complexity to develop and test the framework.

First, the Ethereum blockchain was the first blockchain network to allow the implementation of smart contracts. Since then, the network has been enhanced and widely adopted by different sectors of the economy, companies of vary sizes, academic projects, and more. Together with its community of developers, these contributions over the years built upon Ethereum a credibility status over its workings. So, even though adopting for this project a public network of this size, with its characteristics of full transparency and decentralization, could increase the costs for operating the framework – *and this will be better seen and discussed in Subsection 4.5 and Section 5* –, it brings a more realistic sense of how this framework would work in a real blockchain environment.

Next, the Ethereum community has a considerable size and the documentation available to support the development of smart contracts in their network is abounding. The programming language used for developing smart contracts is Solidity. Although this language is specific, it has a considerable easy learning curve, since it resembles JavaScript.

Lastly, the Remix IDE, an online tool aimed at developing smart contracts on Ethereum network, gives the possibility to not only deploy real smart contracts on the real Ethereum blockchain, but also to run smart contracts on virtual machines with the simplicity of doing everything on a single webpage. This brings to the purpose of this project the celerity and minimum cost needed to test, verify, correct possible mistakes, and run it all over again until the framework is working properly. Since the Remix IDE simulates the Ethereum blockchain, there is no need to set up nodes, a network of computers, or build the groundings of a blockchain network as it would be needed in a private or hybrid blockchains.

Section 5 discusses possible alternatives regarding infrastructure, mining protocols, and architecture in opposition to the one used.

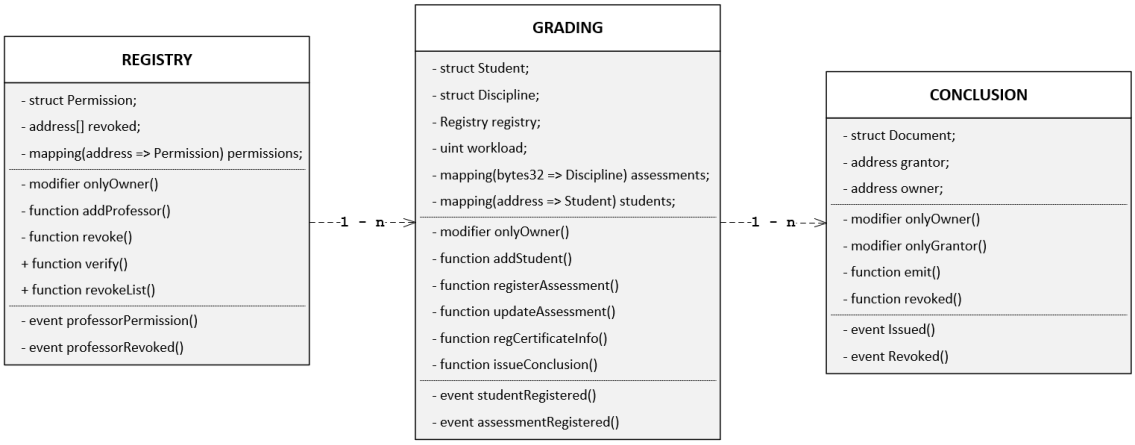

Figure 11 *- Smart contracts class diagrams.*

4.1. SMART CONTRACT 1: REGISTRY

This smart contract is the first deployed in the system. It is responsible for registering the Professor's information that are allowed to interact in the network. Only the HEI can deploy this smart contract in the blockchain. Also, there are two restricted functions, a*ddProfessor* and *revoke*, where HEI is the owner. The last two functions are unrestricted. All four functions are described below (*r* states for restricted, and *ur* states for unrestricted):

addProfessor *(r)***.** register a new professor in the system.

revoke *(r)***.** modify the status of any mapped participant in the system.

verify *(ur)***.** returns a Boolean value when checking a participant status in the system.

revokeList *(ur)***.** returns an array of Ethereum addresses of participants that had been revoked in the system.

To add a Professor in the blockchain, the function *addProfessor* is called by HEI. This function requires the Professor's address in the blockchain and an expiry date as input parameters. If HEI, for some reason, needs to invalidate some of the participants status in the system, function *revoke* is called. To avoid any unauthorized execution of these functions, a modifier called *onlyOwner* is used.

Lastly, it was created two functions for verification purposes. These functions are unrestricted and can be called by anyone in the blockchain. The first one is *verify* and calls for the participants' status. It outputs true if the participant was not revoked previously, and false if it was. Another way it can outputs true is if the expiry date has expired. The second one is *revokeList*. This function returns an array list of all Ethereum addresses revoked in the system upon the call.

The full code can be found in the Appendix section. Figure 12 shows part of the code containing the Professor's struct that will be instanced when its corresponding function is called.

```
1.      struct Permission {
2.        address hash;
3.        uint expiry;
4.        bool revoked;
5.        bool registered;
6.        }
```

Figure 12 *- Code snippet of Professor's struct.*

4.2. SMART CONTRACT 2: GRADING

GRADING is the next smart contract in line for deployment. Although its deployment is restricted to the HEI, the constructor defines a Professor as the owner of the smart contract. It requires as inputs the number of assessments that a student must complete to conclude the discipline, the address of the REGISTRY that was previously deployed, and the address of the Professor that will execute the functions of the new smart contract. There are four functions as described below (*r* states for restricted, and *i* states for internal):

addStudent *(r)***.** enrolls a new student in the system.

registerAssessments *(r)***.** allows to record the assessments.

updateAssessments *(r)***.** registers the student's progress.

issueConclusion *(i)***.** creates a new instance of smart contract after all assessments were concluded.

The first main function, *addStudent*, registers the student based on two parameters, their public address in the blockchain and their identification in a Bytes32 format. Next, *registerAssessments* allows the designated Professor of the discipline to record the assessment types and requires the discipline identification. The third main function is *updateAssessment*, and it is called by the Professor to record each time the students progresses in fulfilling the assessments. Besides, this function automatically verifies whether the student has achieved the number of assessments necessary to conclude the discipline. If this is true, the internal function *issueConclusion* is activated and executed, creating a new instance of smart contract called CONCLUSION.

To avoid any unauthorized execution of these functions, a modifier called *onlyOwner* is also used in this smart contract. In this particular case, another requirement is added to the modifier. Besides only the owner being allowed to execute the functions, its permission also needs not to be expired. The full code is described in the Appendix. Figure 13 and Figure 14 shows, respectively, the struct instantiated for the assessments and the contract's modifier.

```
1.      struct Student {
2.          bytes32 id;
3.          bool registered;
4.          uint accomplished;
5.          mapping(bytes32 => Discipline) credits;
6.          mapping(bytes32 => Document) docs;
7.      }

1.      struct Discipline {
2.          bool accomplished;
3.          bool registered;
4.          uint duration;
5.      }
```

***Figure 13** – The struct for Students and Assessment.*

```
1.    modifier onlyOwner {
2.      require(msg.sender == owner);
3.      require(registry.verify(owner));
4.      _;
5.    }
```

***Figure 14** - GRADING's modifier.*

4.3. SMART CONTRACT 3: CONCLUSION

The last smart contract in the system is responsible for creating the student's conclusion certificate for the discipline they were enrolled. It uses as inputs the student's address and the corresponding Professor's address of the particular discipline. If needed, pedagogical supervisors can check the student's status by finding the CONCLUSION containing the student's address. This means that it can be verified if the certificate has been disabled or if the Professor was unauthorized for any reason. There are two main functions in this smart contract:

issue. emits the conclusion certificate.

destroy. invokes *selfdestruct* function to correct mistakes in the system.

Since this is an ending point in the student progression for completing the discipline, some tool must be available to correct mistaken updates when recording the inputs. An example of wrong doing could be a Professor wrongly recording an assessment credit in GRADING, prompting an anticipated CONCLUSION issuance. Thus, the function *destroy* could be called. This function would disable the smart contract and clear its code and data in the most recent block in the chain. The full code is described in the Appendix. Figure 15 shows the struct instantiated for the conclusion certificates.

```
1.  struct Document {
2.          address issuer;
3.          address receiver;
4.          bytes32 title;
5.          bytes32 description;
6.          uint date;
7.          bool status;
8.      }
9.
```

Figure 15 *- The struct for Certificate.*

4.4. TESTING EXPERIMENT

In this subsection, we walk through the steps of an experiment conducted to validate our proposal. As mentioned in the beginning of this section, we used the Remix IDE running on a Virtual Machine (VM) to deploy and execute the smart contracts. We also compiled our source code on Solidity for version 0.4.24 or higher.

When we first open the Remix running on a VM, a set of 15 accounts with individual addresses are provided, with 100 ethers each and 3MM of gas limit for the account that deploys the smart contract. We selected the address 0x5B38 to represent the HEI in the system. With that so, the first smart contract, REGISTRY, is deployed. Then, the first step is to register a Professor. For that, it requires the Professor's address, a hash value arising from the combination of the HEI and Professor addresses, and a Unix timestamp for the expiry date. This is the main step of this smart contract because only after registering the Professor the next smart contract can be deployed. There are 3 other functions that can be called in this smart contract: *revoke*, which receives as input the Professor's address that the HEI wants to withdraw from the system, and can only be executed by the HEI; *revokeList*, which is a list that shows all the addresses that were revoked; and *verify*, that checks if the address regarding some Professor is registered on the system. Figure 16 illustrates the contract deployed in Remix.

Table 5 shows the information of each transaction of the REGISTRY smart contract. Transaction 1 represent the deployment of an instance of this smart contract by HEI (0x5B38). Next, Transaction 2 represent the execution of *addProfessor* function. It can be seen that the HEI (0x5B38) is requesting the REGISTRY (0x0fC5) to execute the function with the inputs as being: 0xAb84 as the Professor's address; 0x03C6 as the combination's hash; and 1671321599 (17.12.2022 at 23h59m59s) as the expiration date. This information combined registers a new permission representation for this Professor. Before the execution of Transaction 3, another Professor was added with the address 0x1aE0. This was done so it would not interfere with the rest of the experiment using the 0xAb84 as the main address. So, in this transaction, the same from-to was used, but now, as input, it was added the address 0x1aE0. To confirm that the address was added to the revoke list and its revoke status to True, *revokeList* function was called. Its result is also illustrated in Figure 16. Lastly,

Transaction 4 receives as input the address 0xAb84 to verify that it was correctly added to the system.

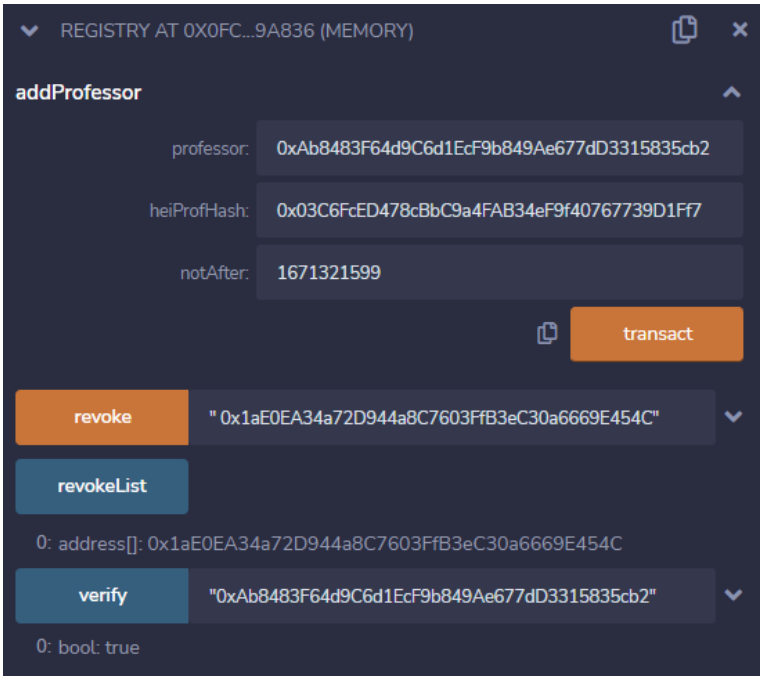

Figure 16 *– Deployed REGISTRY smart contract in Remix IDE.*

Table 5 *– REGISTRY's transactional data.*

TRANSACTION 1: Contract deployment	
status	true Transaction mined and execution succeed
from	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to	Registry.(constructor)
cost	569.231 gas
TRANSACTION 2: *addProfessor* function	
status	true Transaction mined and execution succeed
from	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to	0x0fC5025C764cE34df352757e82f7B5c4Df39A836
cost	93.450 gas
log	"event": "professorPermission", "address professor": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "address heiProfHash": "0x03C6FcED478cBbC9a4FAB34eF9f40767739D1Ff7", "uint256 notAfter": "1671321599"
TRANSACTION 3: *revoke* function	
status	true Transaction mined and execution succeed
from	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to	0x0fC5025C764cE34df352757e82f7B5c4Df39A836
cost	75.506 gas
input	"address professor": "0x1aE0EA34a72D944a8C7603FfB3eC30a6669E454C"
TRANSACTION 4: *verify* function	
status	true Transaction mined and execution succeed
from	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to	0x0fC5025C764cE34df352757e82f7B5c4Df39A836
cost	26.534 gas
input	"address professor": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2"
output	"0": "bool: true"

To deploy the next smart contract, GRADING, some parameters are requested in advance: the number of assessments required to complete the course, which in this example was chosen as 3; the address of the deployed smart contract REGISTRY (0x0fC5); and the address of the Professor previously registered that will be responsible to operate this new smart contract (0xAb84). Figure 17 illustrates this process.

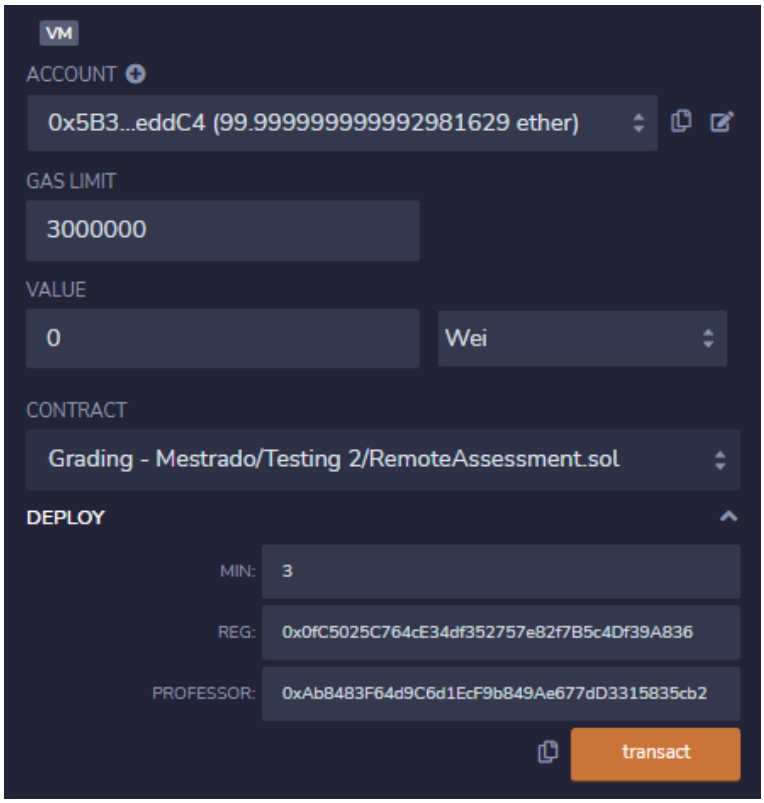

Figure 17 *- Smart contract GRADING to be deployed.*

Now that the contract was deployed, several functions are available for the contract owner (Professor 0xAb84) to execute. Table 6 and Table 7 shows the information for all transactions performed in GRADING. Transaction 5 represent the deployment of an instance of this smart contract by HEI (0x5B38). Next, Transaction 6 represent the execution of *addStudent* function. It can be seen that the Professor (0xAb84) is requesting the GRADING (0x9D83) to execute the function with the inputs as being: 0x7873 as the Student's address; and 0x5061 (Paulo Victor Dias) as the Student's id in Bytes32. Transaction 7 registers an assessment for the course taking as input: an id, in Bytes32, with the value 0x4173 (Assessment n1); and an expiration date, in Unix, 1671321599 (17.12.2022 at 23h59m59s). Transaction 8 updates the Student's progress towards the completion of the discipline. It took as input: the id of the assessment (0x4173); the status of completion (true); and the address of the student that completed this assessment (0x7873). To verify if the subject was correctly assigned to this student and also to follow his/her progress, function *verifyStudent* can be called. Transaction 9 illustrates the information of *updateAssessment* when the Student reaches the number of assessments required to fulfill the discipline and a conclusion certificate is

issued automatically through a third internal smart contract, called CONCLUSION. The arguments passed to the conclusion certificate are: "0" → Issuer; "1" → Receiver; and "2" → Date. The last transaction broken down in the Table 7 references to the function *regCertificateInfo*. This function updates the conclusion certificate of the students with additional information, if the Professor intends to. In this example, the inputs are as follows: a title for the certificate in Bytes32, 0x436f (Conclusion of Discipline n1); a description, also in Bytes 32, 0x4176 (Avg grade: 18); an address for the issuer, 0xAb84; and the address of the student, 0x7873. Figure 18 illustrates the contract deployed in Remix.

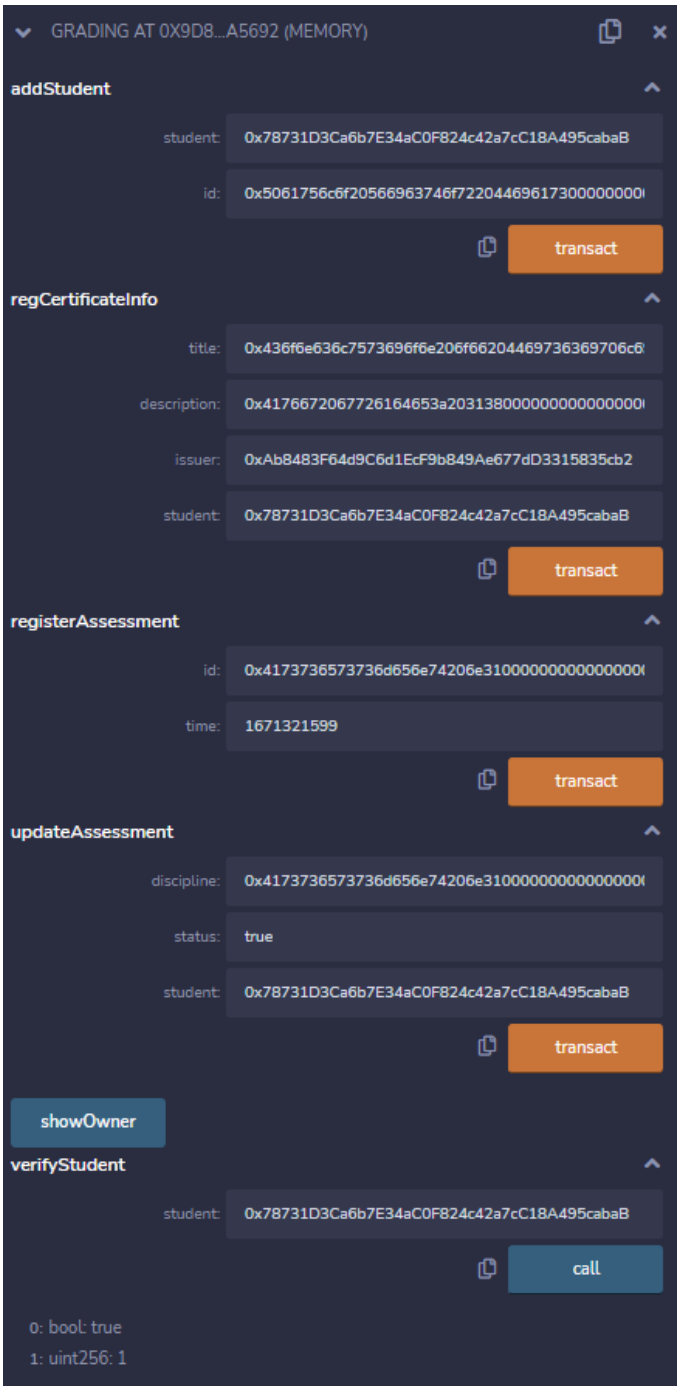

***Figure 18** - Deployed GRADING smart contract in Remix IDE.*

Table 6 *- GRADING's transactional data, part 1.*

TRANSACTION 5: Contract deployment	
status	true Transaction mined and execution succeed
from	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to	Grading.(constructor)
cost	1.395.271 gas
input	"uint256 min": "3", "address reg": "0x0fC5025C764cE34df352757e82f7B5c4Df39A836", "address professor": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2"
TRANSACTION 6: *addStudent* function	
status	true Transaction mined and execution succeed
from	0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2
to	0x9d83e140330758a8fFD07F8Bd73e86ebcA8a5692
cost	83.419 gas
input	"address student": "0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB", "bytes32 id": "0x5061756c6f20566963746f722044696173000000000000000000000000000000"
TRANSACTION 7: *registerAssessment* function	
status	true Transaction mined and execution succeed
from	0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2
to	0x9d83e140330758a8fFD07F8Bd73e86ebcA8a5692
cost	78.887 gas
input	"bytes32 id": "0x4173736573736d656e74206e310000000000000000000000000000000000", "uint256 time": "1671321599"

Table 7 *- GRADING's transactional data, part 2.*

TRANSACTION 8: *updateAssessment* function	
status	true Transaction mined and execution succeed
from	0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2
to	0x9d83e140330758a8fFD07F8Bd73e86ebcA8a5692
cost	86.247 gas
input	"bytes32 discipline": "0x4173736573736d656e74206e3100000000000000000000000000000000000000",
	"bool status": true,
	"address student": "0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB"
TRANSACTION 9: *updateAssessment* function	
status	true Transaction mined and execution succeed
from	0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2
to	0x9d83e140330758a8fFD07F8Bd73e86ebcA8a5692
cost	339.476 gas
input	"bytes32 discipline": "0x4173736573736d656e74206e3100000000000000000000000000000000000000",
	"bool status": true,
	"address student": "0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB"
log	"event": "Issued",
	"args": {
	"0": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2",
	"1": "0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB",
	"2": "1660073337"
	}
TRANSACTION 10: *regCertificateInfo* function	
status	true Transaction mined and execution succeed
from	0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2
to	0x9d83e140330758a8fFD07F8Bd73e86ebcA8a5692
cost	84.066 gas
input	"bytes32 title": "0x436f6e636c7573696f6e206f662044697363697706c696e65206e310000000000",
	"bytes32 description": "0x417667206772616465 3a203138000000000000000000000000000000000000",
	"address issuer": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2",
	"address student": "0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB"

4.5. COST ANALYSIS

Given the results of the experiment discriminated in the previous subsection, it becomes possible to estimate the costs charged by Ethereum to run our prototype in their public blockchain network. We take in consideration the costs related to transactions and execution of the contracts and functions. The scenario to approximate the gas cost necessary to deploy and execute our proposal is: one professor responsible for one discipline, with 20 students, and 3 assessments of the same type, required for each student to fulfil. We also assumed that all students attended the classes and received a conclusion certificate. After the estimation in gas, we present the cost in US$ as well.

Table 8 compiles the gas cost for every transaction executed in the testing experiment. If we deep into the details of the table, it can be noticed that one cost stands out in matters of gas usage, the constructor's deployment. There are a few reasons for that. One is the size of the inputs, which is larger than in the other functions. Furthermore, there are internal variables that are initiated in non-volatile memory that depend on expensive instructions on the Ethereum VM. However, constructors are only instantiated once when the smart contract is deployed, making this cost a one-time paying fee.

Table 8 *– Gas cost of the prototype.*

REGISTRY		**GRADING**		**CONCLUSION**	
Function	**Gas**	**Function**	**Gas**	**Function**	**Gas**
constructor	569.231	*constructor*	1.395.271	*constructor*	278.133
addProfessor	93.450	*addStudent*	83.419		
revoke	75.506	*registerAssessment*	78.887		
verify	26.534	*updateAssessment*	86.247		
		issueConclusion	339.476		
		regCertificateInfo	84.066		

Now, we use these values to estimate how much gas is needed to run our prototype in the scenario abovementioned. The first equation expresses the amount of gas needed to deploy the first smart contract REGISTRY and register the permission for every eligible professor. Then, the second equation represents the cost of deploying instances of GRADING for each Professor. In addition, it is also considering the cost of registering assessments' types for every REGISTRY. Next, the third equation calculate the gas needed to enroll new students to each discipline. The fourth equation calculates the total cost of updating students' progress. Finally, the last equation calculates the total gas consumed for issuing the conclusion certificate for each student. The letters in the equations stands for: P = number of professors; C = number of classrooms; A_T = types of assessments; A_N = number of assessments; S = number of students.

$$Cost_1 = 569.231 + 93.450 \times P \quad (2)$$

$$Cost_2 = P \times (C \times (1.395.271 + (78.887 \times A_T))) \quad (3)$$

$$Cost_3 = S \times 83.419 \quad (4)$$

$$Cost_4 = S \times A_N \times 86.247 \quad (5)$$

$$Cost_5 = S \times 339.476 \quad (6)$$

Using the information of the scenario presented before and applying it to the equations, we arrive at the values of Table 9.

Table 9 *– Gas cost for the presented scenario.*

Equation	Gas
$Cost_1$	662.681
$Cost_2$	1.474.158
$Cost_3$	1.668.380
$Cost_4$	5.174.820
$Cost_5$	6.789.520
Total	**15.769.559**

From the table above, we can take some relevant insights regarding what weights more, in terms of gas consumption, when running our prototype. For an average class with 20 students and 3 assessments of the same type (e.g., two midterm exams and one final exam) for conclusion, we notice that the execution of functions responsible for handling student's data, such as *updateAssessment* and *issueConclusion*, dictate the total cost. The explanation for that relies on the number of times these functions are called. Although they do not require much gas to be individually executed, since they are called several times per student during the semester, its total cost grows proportionally.

To estimate the cost, we sum all the gas needed to register the professor, the students and his or her achievements while he or she completes all assessments, and the gas used to create an instance of CONCLUSION for each student. We took out of the calculation the costs of initially deploying the smart contracts REGISTRY and GRADING, since it would tend to zero as these costs are shared by all students entering and leaving the HEI over the course of time. So, in this proposed condition, the costs per classroom are 13.805.057 gas. According to the current ETH/USD exchange rate, this total amount of gas is equivalent to US$25,189.

$$Total\ Cost(USD) = Total\ Gas * ETH\ Price * 0{,}000000001 \quad (7)$$

$$Total\ Cost(USD) = 13.805.057 * 1.824{,}63 * 0{,}000000001$$

$$Total\ Cost(USD) = 25{,}189\ USD$$

5. DISCUSSION

In this section, we deliberate about possible alternatives regarding infrastructure, mining protocols, and architecture. Discussion about privacy and security matters in relation to our prototype are also put forth.

Our solution uses the Ethereum blockchain which, until the current day, is a public network based on Proof-of-Work mining protocol – *a shadow fork for testing Proof-of-Stake protocol went live on April, 11th of 2022* [96]*; the actual merge is expected to occur between August and November, 2022* [97] – There are other types of blockchain networks available concerning its architecture, to name it: private, hybrid, and public permissioned. Below, we compare them with our actual proposal.

Let's take the private blockchain first. With its implementation, three main attributes could be directly affected: network arrangement, cost, and privacy. Since in a private blockchain all participants are known, mechanisms for authentication and authorization could be done differently. It may not be needed to have a smart contract responsible for validation, and implementing a different consensus protocol could handle this issue. When we attach our solution to a public blockchain, we are bound to its protocols. Alternatively, cryptocurrencies and computational power could be putted aside so a less costly consensus could take place, maybe using stakes or reputation over PoW. Furthermore, since we use Ethereum blockchain, the costs for transaction are charged by the network. Detaching the solution from a real cryptocurrency would definitely lower the cost of implementation. Lastly, private blockchains can decrease privacy issues in exchange of centralization of information and less transparency. Although all stakeholders are referenced by their blockchain addresses, still the information is available in the network. So, lessening the access of what is transacted clearly increases privacy. More in privacy and security is discussed in the next paragraphs.

Hybrid blockchain, or in other words having both public and private blockchains working together, could also be an alternative. A possible solution could work in a way that all transactions with sensible information are made in a private blockchain, and the metadata of these processes could be registered in a public blockchain. This metadata would serve only for the purpose of authenticity validation, without giving access to any sort of identifiers. There are some problems regarding this solution though. First, the complexity for implementing it would raise, consequently raising its cost as well. Then, this also points back to a less decentralized system, since it would be needed a central authority to validate information in the private network and update it to the public.

Public permissioned blockchains provides an environment where a group of participants could be granted different permissions on the network. Some could be granted writing permission while others read only permission. This arrangement could lessen the cost of executing the system because it would

not need a complex validation system with cryptocurrencies or computational power. Hyperledger Fabric [98] could be a good example of blockchain network to make this solution possible. Here, there is still an exchange between full decentralization and transparency, but given the purpose of the system, it may be taken in consideration for future improvement to test this framework in the Hyperledger Fabric and compare results for full optimization.

Following, we discuss about privacy and security matters that may derive from this work. When concerning about privacy issues, it should be taken into account if private information about the stakeholders is somehow being disclosed. When recording the student's progress in the system, no grades nor other personal identifiable information is being uploaded. What the framework records is how many assessments have been accomplished until it publishes the completion of the subject that the student was pursuing. Also, all students are identified in the blockchain by their public key. So, even though these data go to the system, there is no way to correlate them with a student. Some students may still find that they want to have more power towards what is disclosed or not regarding their academic progress. For this, some changes may be needed in the framework. Changing it to a public permissioned blockchain and adding some mechanisms that gives the students the possibility to choose what to disclose or not may steer towards this objective.

Security affairs are another crucial aspect of the framework well-functioning. For that, it should be looked how each stakeholder takes part in the system and how could they maliciously interfere. Let's start analyzing the by the student's perspective. Students have no access to smart contracts; this is the professor's whole. Thus, no student can intentionally harm or interfere in the system. Next, the professor's perspective. They have the authority to register the assessments and update student's information to the blockchain. No professor can access other professor's discipline since each smart contract is individually owned by them. A professor can deliberately provide fake information about the progress of a specific student. This cannot be prevented but can be easily identified by auditing the transactions a professor maliciously filled in the smart contracts. Also, the professors are hold accountable for their transactions in the blockchain, hindering misconducts by their part. If this happens anyway, the smart contract can be disabled by removing the conclusion's certificate, if that is the case. Lastly, the HEI's part in the system. They are the most interested in stablishing the correct usage of the system. They are responsible for registering the participants and deploying the smart contracts, but cannot interfere in the updates of the assessments. Therefore, they cannot surpass the professor's authority in the process. If the HEI's credential is compromised, they should notify the event and put on suspicion all smart contracts created since then.

6. CONCLUSION

The COVID-19 outbreak brought a new attention to a topic that it was already building its way, although in relative slow steps: remote education. The boom on the online platforms to fulfill the problems with in-person education also shed light to the vulnerabilities of the actual systems regarding personal data, security in assessments and the discrepancy of access and solutions between HEIs.

In this research work, it was proposed the application of a blockchain-based framework in the process of reliability and validation of information exchanged between students and educational institutions in order to mitigate plagiarism or e-cheating factors. A review of the concepts of distance learning together with existing conventional frameworks and potential solutions utilizing blockchain-based technology were exposed. Challenges in remote assessment also were deep looked into. Aspects of cheating and plagiarism were analyzed by the student and institution's view, and the correlation between face-to-face and distance learning. Solutions for this problem were also analyzed by conventional and blockchain-based platforms. Regarding the aspects of security and safety, the research showed that the combination of blockchain and e-learning can pave the way to solve most of the current issues, due to blockchain's ability to transmit data across a vast network and its information security.

The framework proposed was designed as a blockchain infrastructure and a set of smart contracts to record academic progress and issue conclusion certificates of discipline completion in a transparent and automated manner. It encompasses a variety of tools to support the goal of mitigating academic dishonesty in online evaluations. It combines cryptographic pair keys for all participants to enhance authenticity of the actions performed in the system, it uses antiplagiarism tools for validation of the works delivered by the students, and smart contracts to automate processes and reduce human interference. In Chapter 3, we presented in details the prototype, with the description of the participants, an execution experiment, and a cost evaluation for implementing the system.

Looking from the cost perspective, the system shows a limitation for a real implementation. Using a public blockchain of the size of Ethereum brings several advantages such as decentralization and authority-free operation, but also carries the costs for this to work. Having to run a framework that needs recurrent updates depending on a volatile cryptocurrency would bring difficulty to the HEIs to project the costs of using the system per semester. Even with the currently value of ETH, the total cost calculated would become impractical for most part of the HEIs.

In essence, the developed framework met the desired proposal, fulfilling its purpose of delivering a safer network for improving the integrity of data, the authenticity of the participants involved, and the validation of the assessments' accomplished conductive to a lower rate of e-cheating or plagiarism.

7. FUTURE WORK

Future improvements to this proposal may consider the implementation of plagiarism detection tools to be activated automatically by a smart contract, accepting or rejecting the submission depending on a certain acceptable percentage determined by the academic board. Also, migrating the system from the Ethereum blockchain to a public permissioned blockchain, such as Hyperledger Fabric, may be more suitable for the nature of the project. It would dissociate the system from cryptocurrencies expenditures, potentially reducing the cost of the system. Another advantage would the possibility to implement autonomy tools for students regarding what should or should not be disclosed to public scrutiny. Lastly, It would be also interesting to implement the proposed framework in a real environment or with real data to validate the solution in a more reliable way.

REFERENCES

[1] P. Leviäkangas, "Digitalisation of Finland's transport sector," *Technology in Society,* vol. 47, pp. 1-15, 2016.

[2] M. Marjani, F. Nasaruddin, A. Gani, A. Karim, I. A. T. Hashem, A. Siddiqa and I. Yaqoob, "Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges," *IEEE Access,* vol. 5, pp. 5247-5261, 2017.

[3] D. E. O'Leary, "Artificial Intelligence and Big Data," *IEEE Intelligent Systems,* vol. 28, no. 2, pp. 96-99, 2013.

[4] A. Sestino, M. I. Prete, L. Piper and G. Guido, "Internet of Things and Big Data as enablers for business digitalization strategies," *Technovation,* vol. 98, 2020.

[5] D. Ibarra, J. Ganzarain and J. I. Igartua, "Business model innovation through Industry 4.0: A review," *Procedia Manufacturing,* vol. 22, pp. 4-10, 2018.

[6] S. Likens, "Eight emerging technologies and six convergence themes you need to know about," PwC, 12 Jan 2022. [Online]. Available: https://www.pwc.com/us/en/tech-effect/emerging-tech/essential-eight-technologies.html. [Accessed 23 Fev 2022].

[7] R. Geissbauer, S. Schrauf, V. Koch and S. Kuge, "Industry 4.0 - Opportunities and Challanges of the Industrial Internet," PricewaterhouseCoopers Aktiengesellschaft Wirtschaffsprufungsgesellschaft, 2014.

[8] I. Dobre, "Learning Management Systems for Higher Education - An Overview of Available Options for Higher Education Organizations," *Procedia - Social and Behavioral Sciences,* vol. 180, pp. 313-320, 2015.

[9] A. Aldiab, H. Chowdhury, A. Kootsookos, F. Alam and H. Allhibi, "Utilization of Learning Management Systems (LMSs) in higher education system: A case review for Saudi Arabia," *Energy Procedia,* vol. 160, pp. 731-737, 2019.

[10] J. Reich and J. A. Ruipérez-Valiente, "The MOOC pivtot," *Science,* vol. 363, no. 6423, pp. 130-131, 2019.

[11] J. Reich, "MOOC Completion and Retention in the Context of Student Intent," Educase Review, 08 Dec 2014. [Online]. Available: https://er.educause.edu/articles/2014/12/mooc-completion-and-retention-in-the-context-of-student-intent. [Accessed 11 Jan 2022].

[12] World Health Organization, "WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020," World Health Organization (WHO), 11 Mar 2020. [Online]. Available: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020. [Accessed 11 Jan 2022].

[13] B. Evans, "https://accelerationeconomy.com/cloud/the-zoom-revolution-10-eye-popping-stats-from-techs-new-superstar/," Acceleration Economy Network, 04 Jun 2020. [Online]. Available: https://accelerationeconomy.com/cloud/the-zoom-revolution-10-eye-popping-stats-from-techs-new-superstar/. [Accessed 11 Jan 2022].

[14] V. Vaitheeswaran, "Covid-19 forced businesses to experiment," The Economist, 16 Nov 2020. [Online]. Available: https://www.economist.com/the-world-ahead/2020/11/16/covid-19-forced-businesses-to-experiment. [Accessed 11 Jan 2022].

[15] UNESCO, "Education: From disruption to recovery," UNESCO, [Online]. Available: https://en.unesco.org/covid19/educationresponse. [Accessed 11 Jan 2022].

[16] ReportLinker, "Global Mobile Learning Industry," Global News Wire, 18 Aug 2020. [Online]. Available: https://www.globenewswire.com/news-release/2020/08/18/2080347/0/en/Global-Mobile-Learning-Industry.html. [Accessed 2022 Fev 23].

[17] S. Johnes, "The Impact Of Blockchain Technology On The eLearning Industry," eLearning Industry, 07 Nov 2021. [Online]. Available: https://elearningindustry.com/impact-of-blockchain-technology-on-the-elearning-industry. [Accessed Fev 23 2022].

[18] M. Killeen, "Privacy concerns set to grow with the digitalisation of education," Euractiv, 30 Jul 2021. [Online]. Available: https://www.euractiv.com/section/digital/news/privacy-concerns-set-to-grow-with-the-digitalisation-of-education/. [Accessed 24 Fev 2022].

[19] O. L. Holden, M. E. Norris and V. A. Kuhlmeier, "Academic Integrity in Online Assessment: A Research Review," *Frontiers in Education,* vol. 6, 2021.

[20] L. Ante, "Smart contracts on the blockchain – A bibliometric analysis and review," *Telematics and Informatics,* 16 Oct 2020.

[21] A. Hevner and S. Chatterjee, Design Research in Information Systems: Theory and Practice, vol. 22, Springer Science & Business Media, 2010, p. 320.

[22] OECD, "E-learning in Tertiary Education," *OECD Observer,* pp. 1-8, Dec 2005.

[23] C. Heitz, M. Laboissiere, S. Sanghvi and J. Sarakatsannis, "Getting the next phase of remote learning right in higher education," McKinsey, 23 Apr 2020. [Online]. Available: https://www.mckinsey.com/industries/education/our-insights/getting-the-next-phase-of-remote-learning-right-in-higher-education. [Accessed 13 Jan 2022].

[24] J. Simon, "What is Distance Learning? The Complete Guide (2021)," TechSmith, [Online]. Available: https://www.techsmith.com/blog/distance-learning/. [Accessed 13 Jan 2022].

[25] S. Hrastinski, "Asynchronous and Synchronous E-Learning," *EDUCAUSE Review,* 17 Nov 2008.

[26] A. M. Kaplan and M. Haenlein, "Higher education and the digital revolution: About MOOCs, SPOCs, social media, and the Cookie Monster," *Business Horizons,* vol. 59, no. 4, pp. 441-450, 2016.

[27] N. Cavus, "Distance Learning And Learning Management Systems," *ScienceDirect,* vol. 191, pp. 872-877, 2015.

[28] F. L. Matucheski and P. T. Lupion, "Potencialidades e limitações do ambiente virtual de aprendizagem em um curso online," *Revista Intersaberes,* vol. 5, no. 10, pp. 152-166, 2010.

[29] P. C. de Oliveira, C. J. C. d. A. Cunha and M. K. Nakayama, "Learning Management Systems (LMS) and E-Learning Management: An Integrative Review and Research Agenda," *Journal of Information Systems and Technology Management (JISTEM),* Aug 2016.

[30] N. Cavus, "The evaluation of Learning Management Systems using an artificial intelligence fuzzy logic algorithm," *Advances in Engineering Software,* vol. 41, no. 2, pp. 248-254, 2010.

[31] UNESCO, "Distance learning solutions," UNESCO, [Online]. Available: https://en.unesco.org/covid19/educationresponse/solutions. [Accessed 13 Jan 2022].

[32] F. P. Oganda, N. Lutfiani, Q. Aini, U. Rahardja and A. Faturahman, "Blockchain Education Smart Courses of Massive Online Open Course Using Business Model Canvas," *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS),* pp. 1-6, 2020.

[33] T. Y. Lam and B. Dongol, "A blockchain-enabled e-learning platform," *Interactive Learning Environments,* pp. 1-23, 03 Feb 2020.

[34] A. Garg, S. A, P. Kumar, M. Madhukar, O. Loyola-González and M. Kumar, "Blockchain-based online education content ranking," *Education and Information Technologies,* 15 Nov 2021.

[35] V. Arkorful and N. Abaidoo, "The role of e-learning, advantages and disadvantages of its adoption in higher education," *International Journal of Instructional Technology and Distance Learning,* pp. 29-42, Jan 2015.

[36] M. Mohamed and A. Shaikha, "Whither plagiarism in distance learning academic assessment during COVID-19?," *2020 Sixth International Conference on e-Learning (econf),* pp. 1-5, 2020.

[37] S. Kocdar, A. Karadeniz, R. Peytcheva-Forsyth and V. Stoeva, "Cheating and plagiarism in e-assessment: Students' perspectives," *Open Praxis,* vol. 10, no. 3, pp. 221-235, 2018.

[38] The Editors of Encyclopaedia Britannica, "Student's t-test," Britannica, [Online]. Available: https://www.britannica.com/science/Students-t-test. [Accessed 21 Jun 2022].

[39] S. Glen, "ANOVA Test: Definition, Types, Examples, SPSS," StatisticsHowTo.com: Elementary Statistics for the rest of us!, [Online]. Available: https://www.statisticshowto.com/probability-and-statistics/hypothesis-testing/anova/. [Accessed 21 Jun 2022].

[40] J. Levine and V. Pazdernik, "Evaluation of a four-prong anti-plagiarism program and the incidence of plagiarism: a five-year retrospective study," *Assessment & Evaluation in Higher Education,* vol. 43, no. 7, pp. 1094-1105, 2018.

[41] C. Li, J. Guo, G. Zhang, Y. Wang, Y. Sun and B. Rongfang, "A Blockchain System for E-Learning Assessment and Certification," *2019 IEEE International Conference on Smart Internet of Things (SmartIoT),* pp. 212-219, 9-11 Aug 2019.

[42] N. Jing, Q. Liu and V. Sugumaran, "A blockchain-based code copyright management system," *Information Processing & Management,* vol. 58, no. 3, 2021.

[43] J. Hoffstein, J. Pipher and J. H. Silverman, An Introduction to Mathematical Cryptography, New York: Springer, 2008, pp. XVI, 524.

[44] "Secure Hash Signature Standard (SHS) (FIPS PUB 180-2).". United States Patent Federal Information Processing Standard (FIPS) 180-2, 2002.

[45] G. Bertoni, J. Daemen, S. Hoffert, M. Peeters, G. Van Assche and R. Van Keer, Keccak Team, [Online]. Available: https://keccak.team/index.html. [Accessed 10 04 2022].

[46] E. Paul, "What is Digital Signature: How it works, benefits, objectives, concept," EMP Trust HR, 12 Sep 2017. [Online]. Available: http://www.emptrust.com/blog/benefits-of-using-digital-signatures/. [Accessed 10 Apr 2022].

[47] "Infraestrutura da Chave Pública (PKI)," IBM, 20 Apr 2021. [Online]. Available: https://www.ibm.com/docs/pt-br/ibm-mq/8.0?topic=ssfksj-8-0-0-com-ibm-mq-sec-doc-q009900--htm. [Accessed 10 Apr 2022].

[48] "Medida Provisória n 2.200-2," Presidência da República - Casa Civil - Subchefia para Assuntos Jurídicos, 24 Aug 2001. [Online]. Available: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. [Accessed 10 Apr 2022].

[49] "Decreto-Lei n.º 290-D/99 de 2 de Agosto," Ministério da Ciência e da Tecnologia, [Online]. Available: https://www.igf.gov.pt/leggeraldocs/DL_290_D_99.htm#:~:text=1%20%2D%20O%20presente%20diploma%20regula,id%C3%AAnticas%20%C3%A0s%20da%20assinatura%20digital.. [Accessed 10 Apr 2022].

[50] M. D'Aliessi, "How Does the Blockchain Work?," OneZero, 01 Jun 2016. [Online]. Available: https://onezero.medium.com/how-does-the-blockchain-work-98c8cd01d2ae. [Accessed 10 Apr 2022].

[51] A. M. d. Morais and F. A. A. Lins, "Uso de Blockchain na Educação: Estado da arte e desafios em aberto," *Revista Científica Multidisciplinar Núcleo do Conhecimento,* vol. 22, no. 10, pp. 78-100, 2020.

[52] M. Turkanovic, M. Hölbl, K. Kosic, M. Hericko and A. Kamisalic, "EduCTX: A Blockchain-Based Higher Education Credit Platform," *IEEE Access,* p. 16, 2018.

[53] Cryptopedia Staff, "Cryptopedia," Gemini, 22 July 2021. [Online]. Available: https://www.gemini.com/cryptopedia/blockchain-types-pow-pos-private. [Accessed 14 December 2021].

[54] A. Takyar, "Proof of Work vs. Proof of Stake: An In-Depth Discussion," DZone, 27 Aug 2019. [Online]. Available: https://dzone.com/articles/the-proof-of-work-vs-proof-of-stake-an-in-depth-di. [Accessed 21 Jun 2022].

[55] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," bitcoin.org, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed 16 Fev 2022].

[56] R. C. Merkle, "Method of providing digital signatures". USA Patent US4200770A, 05 May 1979.

[57] D. L. Chaum, *Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups,* California: University of California, Berkeley, 1982.

[58] A. T. Sherman, F. Javani, H. Zhang and E. Golaszewski, "On the Origins and Variations of Blockchain Technologies," *IEEE Security Privacy,* vol. 17, no. 1, pp. 72-77, 2019.

[59] S. Haber and W. S. Stornetta, "How To Time-Stamp a Digital Document," *Journal of Cryptology,* pp. 99-111, 1991.

[60] S. Haber, W. S. Stornetta and D. Bayer, "Improving the Efficiency and Reliability of," 1992.

[61] C. H. Ding, S. Nutanong and R. Buyya, *P2P Networks for Content Sharing,* Melbourne, 2004.

[62] A. Back, "Hashcash," hascash, Mar 1997. [Online]. Available: http://www.hashcash.org/papers/. [Accessed 19 Fev 2022].

[63] A. Back, "Hashcash - A Denial of Service Counter-Measure," 2002.

[64] H. Finney, "Satoshi Nakamoto Institute," 2004. [Online]. Available: https://nakamotoinstitute.org/finney/rpow/. [Accessed 19 Fev 2022].

[65] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[66] "Bitcoin: $1bn seized from Silk Road account by US government," BBC News, 05 Nov 2020. [Online]. Available: https://www.bbc.com/news/technology-54833130. [Accessed 19 Fev 2022].

[67] V. Buterin, "A Next Generation Smart Contract and Decentralized," 2013.

[68] J. Evans, "Vapor No More: Ethereum Has Launched," TechCrunch+, 01 Aug 2015. [Online]. Available: https://techcrunch.com/2015/08/01/vapor-no-more-ethereum-has-launched/. [Accessed 19 Fev 2022].

[69] S. Davis, H. Arslanian, D. Fong, A. Watkins, W. Gee and C. Y. Cheung, "Blockchain is here. What's your next move?," PwC, 2018.

[70] I. Intelligence, "The growing list of applications and use cases of blockchain technology in business and life," Business Insider, 10 Feb 2022. [Online]. Available: https://www.businessinsider.com/blockchain-technology-applications-use-cases. [Accessed 19 Feb 2022].

[71] T. Wijman, "The World's 2.7 Billion Gamers Will Spend $159.3 Billion on Games in 2020; The Market Will Surpass $200 Billion by 2023," Newzoo, 08 May 2020. [Online]. Available: https://newzoo.com/insights/articles/newzoo-games-market-numbers-revenues-and-audience-2020-2023/. [Accessed 19 Feb 2022].

[72] P. G. P. &. Utilities, "Blockchain - an opportunity for energy producers and consumers," 2015.

[73] 101 Blockchains, "101 Blockchains," 2 September 2018. [Online]. Available: https://101blockchains.com/blockchain-digital-transformation/. [Accessed 14 December 2021].

[74] M.-F. Steiu, "Blockchain in education: Opportunities, applications, and challenges," *First Monday,* vol. 25, no. 9, 7 September 2020.

[75] A. Grech and A. F. Camilleri, "Blockchain in Education," 2017.

[76] G. Grolleau, Lakhal and N. Mzoughi, "An introduction to the Economics of Fake Degrees," *Journal of Economic Issues,* vol. 42, pp. 673-693, September 2008.

[77] DCC, "Digital Credentials Consortium," DCC, [Online]. Available: https://digitalcredentials.mit.edu/. [Accessed 12 Jan 2022].

[78] Blockcerts, "Blockcerts - The Open Standard For Blockchain Credentials," Blockcerts, [Online]. Available: https://www.blockcerts.org/. [Accessed 12 Jan 2022].

[79] K. H. Duffy and N. Smolenski, "The Time for Self-Sovereign Identity is Now," 07 Nov 2017. [Online]. Available: https://medium.com/learning-machine-blog/the-time-for-self-sovereign-identity-is-now-222aab97041b. [Accessed 12 Jan 2022].

[80] A. R. Bartolomé, C. Bellver, L. Castañeda and J. Adell, "Blockchain in Education: Introduction and Critical Review of the State of the Art," *Revista Electrónica de Tecnología Educativa,* vol. 61, p. 14, 2017.

[81] U. o. Nicosia, "Blockchain Programs," UNIC, [Online]. Available: https://www.unic.ac.cy/blockchain/. [Accessed 12 Jan 2022].

[82] T. T. Huynh, T. Tru Huynh, D. K. Pham and A. Khoa Ngo, "Issuing and Verifying Digital Certificates with Blockchain," *2018 International Conference on Advanced Technologies for Communications (ATC),* pp. 332-336, 2018.

[83] V. Langard, "BCDiploma raises €1.2 million to become the global standard for certifying diplomas and certificates online," 23 May 2019. [Online]. Available: https://medium.com/bcdiploma/bcdiploma-raises-1-2m-58cdba9b3b85. [Accessed 12 Jan 2022].

[84] BCDiploma, "What is a blockchain digital credential?," BCDiploma, [Online]. Available: https://www.bcdiploma.com/en/howItWorks. [Accessed 12 Jan 2022].

[85] W. Gräther, S. Kolvenbach, R. Ruland, J. Schütte, C. Torres and F. Wendland, "Blockchain for Education: Lifelong Learning Passport," *European Society for Socially Embedded Technologies (EUSSET),* vol. 2, no. 10, p. 8, 2018.

[86] Q. Liu, Q. Guan, X. Yang, H. Zhu, G. Green and S. Yin, "Education-Industry Cooperative System Based on Blockchain," *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN),* pp. 207-211, 2018.

[87] J. Zhong, H. Xie, D. Zou and W. K. Chui, "A Blockchain Model for Word-Learning Systems," *5th International Conference on Behavioral, Economic, and Socio-Cultural Computing (BESC),* pp. 130-131, Nov 2018.

[88] BitDegree, "Crypto Is The New Digital, Learn It!," BitDegree, [Online]. Available: https://www.bitdegree.org/. [Accessed 12 Jan 2022].

[89] ODEM, "Learn what inspires you. At your pace, any place, any time.," ODEM, [Online]. Available: https://odem.cloud/. [Accessed 12 Jan 2022].

[90] P. Ocheja, B. Flanagan and H. Ogata, "Connecting decentralized learning records: a blockchain based learning analytics platform," *Proceedings of the 8th International Conference on Learning Analytics and Knowledge,* pp. 265-269, Mar 2018.

[91] J. Rooksby and K. Dimitrov, "Trustless education? A blockchain system for university grades," *Ubiquity: The Journal of Pervasive Media,* vol. 6, no. 1, pp. 83-88, Nov 2019.

[92] S. Gilda and M. Mehrotra, "Blockchain for Student Data Privacy and Consent," *2018 International Conference on Computer Communication and Informatics (ICCCI),* pp. 1-5, 2018.

[93] M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform," *IEEE Access,* vol. 6, pp. 5112-5127, 2018.

[94] "Solidity," Solidity Org, [Online]. Available: https://soliditylang.org/. [Accessed 09 Jun 2022].

[95] "Remix Project," Ethereum Foundation, [Online]. Available: https://remix-project.org/. [Accessed 09 Jun 2022].

[96] D. Thomas and R. James, "First Shadow Fork Goes Live on Ethereum Ahead of Proof-of-Stake Testing," be[in]crypto, 11 Apr 2022. [Online]. Available: https://beincrypto.com/first-shadow-fork-goes-live-on-ethereum-ahead-of-proof-of-stake-testing/. [Accessed 16 Jun 2022].

[97] T. Beiko, Interviewee, *Community Manager at Ethereum Foundation.* [Interview]. 07 Jun 2022.

[98] Hyperledger, "Linux Foundation's Hyperledger Project Announces 30 Founding Members and Code Proposals To Advance Blockchain Technology," The Linux Foundation, 09 Feb 2016. [Online]. Available: https://www.hyperledger.org/announcements/2016/02/09/linux-foundations-hyperledger-project-announces-30-founding-members-and-code-proposals-to-advance-blockchain-technology. [Accessed 19 Jun 2022].

APPENDIX

This chapter attaches the complete set of source codes for the smart contracts developed for the prototype. It can be implemented for Solidity versions from 0.4.24 or higher.

```
1.  pragma solidity ^0.4.24;
2.
3.  //library to hold the structs of the framework
4.  library Structs {
5.
6.      //struct for Professor's permission
7.      struct Permission {
8.        address hash;
9.        uint expiry;
10.       bool revoked;
11.       bool registered;
12.       }
13.
14.     //struct for discipline registration
15.     struct Discipline {
16.         bool accomplished;
17.         bool registered;
18.         uint duration;
19.     }
20.
21.     //struct for Student's registration and progress
22.     struct Student {
23.         bytes32 id;
24.         bool registered;
25.         uint accomplished;
26.         mapping(bytes32 => Discipline) credits;
27.         mapping(bytes32 => Document) docs;
28.     }
29.
30.     //struct for conclusion certificates
31.     struct Document {
32.         address issuer;
33.         address receiver;
34.         bytes32 title;
35.         bytes32 description;
36.         uint date;
37.         bool status;
38.     }
39.
40. }
41.
```

Figure 19 *- Solidity code for Library of Structs.*

```
1.  pragma solidity ^0.4.24;
2.
3.  //import of struct's library
4.  import "./Structs.sol";
5.
6.  contract Registry {
7.
8.      //variables declaration
9.      address private owner;
10.     address[] private revoked;
11.
12.     //mapping Professor's address with permission
13.     mapping(address => Structs.Permission) private permissions;
14.
15.     //modifier declaration for contract owner
16.     modifier onlyOwner {
17.       require(msg.sender == owner);
18.       _;
19.     }
20.
21.     //setting contract owner when contract is deployed
22.     constructor() public {
23.       owner = msg.sender;
24.     }
25.
26.     //event to log when a permission is issued
27.     event professorPermission(address from, address to, uint date);
28.
29.     //function to register Professor's permission in the system
30.     function addProfessor(address professor, address heiProfHash, uint
    notAfter) public onlyOwner {
31.       require(professor != 0x0);
32.       permissions[professor].hash = heiProfHash;
33.       permissions[professor].expiry = notAfter;
34.       permissions[professor].revoked = false;
35.       permissions[professor].registered = true;
36.       emit professorPermission(owner, professor, now);
37.     }
38.
39.     //event to log when a permission is revoked
40.     event professorRevoked(address from, address to, uint date);
41.
42.     // function to revoke Professor's permission in the system
43.     function revoke(address professor) public onlyOwner {
44.       require(professor != 0x0 && permissions[professor].registered);
45.       permissions[professor].revoked = true;
46.       revoked.push(professor);
47.       emit professorRevoked(owner, professor, now);
48.     }
49.
50.     //function to verify if Professor is registered in the system
51.     function verify(address professor) public constant returns(bool) {
52.       require(professor != 0x0 && permissions[professor].registered);
53.       if(permissions[professor].revoked || permissions[professor].expiry <
    now) {
54.         return false;
55.       }
56.       return true;
57.     }
58.
59.     // function to list all revoked addresses
60.     function revokeList() external constant returns(address[]) {
61.       return revoked;
62.     }
63. }
64.
```

Figure 20 *– Solidity code for smart contract REGISTRY.*

```
1.  pragma solidity ^0.4.24;
2.
3.  //import of struct's library
4.  import "./Structs.sol";
5.
6.  contract Grading {
7.
8.    //variables declaration
9.    address private owner;
10.   Registry private registry; //importing functions from REGISTRY smart
    contract
11.   uint private workload;
12.
13.   //mapping Student's info with discipline and student structs
14.   mapping(bytes32 => Structs.Discipline) private assessments;
15.   mapping(address => Structs.Student) private students;
16.
17.   //modifier declaration for setting Professor as contract owner
18.   modifier onlyOwner {
19.     require(msg.sender == owner);
20.     require(registry.verify(owner));
21.     _;
22.   }
23.
24.   //setting contract owner, registering number of assessments, and REGISTRY
    address when contract is deployed
25.   constructor(uint min, address reg, address professor) public {
26.     require(reg != 0x0 && professor != 0x0);
27.     workload = min;
28.     registry = Registry(reg);
29.     owner = professor;
30.   }
31.
32.   //event to log when a student is registered
33.   event studentRegistered(address from, address to, uint date);
34.
35.   //function to register Student in the system
36.   function addStudent(address student, bytes32 id) public onlyOwner {
37.     require(student != 0x0 && !students[student].registered);
38.     students[student].id = id;
39.     students[student].registered = true;
40.     students[student].accomplished = 0;
41.     emit studentRegistered(owner, student, now);
42.   }
43.
44.   //event to log when an assessment is registered
45.   event assessmentRegistered(address from, address to, uint date);
46.
47.   //function to register an assessment in the system
48.   function registerAssessment(bytes32 id, uint time) public onlyOwner {
49.     assessments[id].registered = true;
50.     assessments[id].duration = time;
51.   }
52.
53.   //function to update Student's progress in the system
54.   function updateAssessment(bytes32 discipline, bool status, address
    student) public onlyOwner {
55.     require(student != 0x0 && students[student].registered &&
    assessments[discipline].registered);
56.     students[student].credits[discipline].accomplished = status;
57.     if(status){
58.       students[student].accomplished += 1;
59.     }
60.     if(students[student].accomplished == workload){
61.       issueConclusion(student);
62.     }
63.   }
64.
65.
```

```
66.
67.   //function to register additional info for certificates in the system
68.   function regCertificateInfo(bytes32 title, bytes32 description, address
    issuer, address student) public onlyOwner {
69.     require(student != 0x0 && students[student].registered && issuer !=
    0x0);
70.     require(registry.verify(issuer));
71.     students[student].docs[title].title = title;
72.     students[student].docs[description].description = description;
73.   }
74.
75.   //internal function to call CONCLUSION when criteria is met
76.   function issueConclusion(address student) internal {
77.     require(registry.verify(owner));
78.     Conclusion conclusion = new Conclusion(student, owner);
79.     conclusion.emit();
80.   }
81.
82. }
83.
```

Figure 21 *- Solidity code for smart contract GRADING.*

```
1.  pragma solidity ^0.4.24;
2.
3.  //import of struct's library
4.  import "./Structs.sol";
5.
6.  contract Conclusion {
7.
8.      //variables declaration
9.      address private grantor;
10.     address private owner;
11.
12.     //registering info in Document struct
13.     Structs.Document private conclusion;
14.
15.     //modifier declaration for setting certificate grantor
16.     modifier onlyGrantor {
17.         require(msg.sender == grantor);
18.         _;
19.     }
20.
21.     //modifier declaration for setting certificate owner
22.     modifier onlyOwner {
23.         require(msg.sender == owner);
24.         _;
25.     }
26.
27.     //setting owner, grantor, and certificate info when contract is deployed
28.     constructor (address st, address inst) public {
29.         require(st != 0x0 && inst != 0x0);
30.
31.         conclusion.receiver = st;
32.         conclusion.issuer = inst;
33.         owner = st;
34.         grantor = inst;
35.     }
36.
37.     //event to log when a certificate is issued
38.     event Issued(address from, address to, uint date);
39.
40.     //function to issue conclusion certificate in the system
41.     function emit() public {
42.         conclusion.date = now;
43.         conclusion.status = true;
44.         emit Issued(conclusion.issuer, conclusion.receiver,
    conclusion.date);
45.     }
46.
47.     //event to log when a certificate is revoked
48.     event Revoked(address from, uint date);
49.
50.     //function to revoke conclusion certificate
51.     function revoked() public onlyGrantor {
52.         selfdestruct(grantor);
53.         emit Revoked(grantor, now);
54.     }
55.
56. }
57.
```

Figure 22 *- Solidity code for smart contract CONCLUSION.*