Verification of University Student and Graduate Data using Blockchain Technology

Article *in* International Journal of Computers, Communications & Control (IJCCC) · September 2021

DOI: 10.15837/ijccc.2021.5.4266

CITATIONS
33

READS
2,169

5 authors, including:

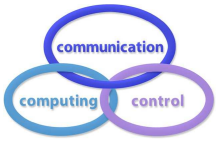
Bolatzhan Kumalakov
Astana IT University
17 PUBLICATIONS **66** CITATIONS
SEE PROFILE

Galimkair Mutanov
Institute of Information and Computing Technologies
47 PUBLICATIONS **183** CITATIONS
SEE PROFILE

Zhanl Mamykova
10 PUBLICATIONS **118** CITATIONS
SEE PROFILE

Ye.I. Kistaubayev
Шымкентский университет
4 PUBLICATIONS **52** CITATIONS
SEE PROFILE

INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
Online ISSN 1841-9844, ISSN-L 1841-9836, Volume: 16, Issue: 5, Month: October, Year: 2021
Article Number: 4266, https://doi.org/10.15837/ijccc.2021.5.4266



CCC Publications

Verification of University Student and Graduate Data using Blockchain Technology

Y. Shakan, B. Kumalakov, G. Mutanov, Zh. Mamykova, Y. Kistaubayev

Yassynzhan Shakan, Galimkair Mutanov*, Zhanl Mamykova, Yerlan Kistaubayev
Al-Farabi Kazakh National University
71 Al-Farabi ave., Almaty, Kazakhstan
*Corresponding author: Mutanov@kaznu.kz
E-mail: shakan_yassynzhan@live.kaznu.kz, zhanl.mamykova@kaznu.kz, erlan.kistaubayev@kaznu.kz

Bolatzhan Kumalakov
Astana IT University,
Block C1, Expo business centre, Turkestan street, Nur-Sultan, Kazakhstan
E-mail: bolatzhan.kumalakov@astanait.edu.kz

Abstract

Blockchain is a reliable and innovative technology that harnesses education and training through digital technologies. Nonetheless, it has been still an issue keeping track of student/graduate academic achievement and blockchain access rights management. Detailed information about academic performance within a certain period (semester) is not present in the official education documents. Furthermore, academic achievement documents issued by institutions are not secured against unauthorized changes due to the involvement of intermediaries. Therefore, verification of official educational documents has become a pressing issue owing to the recent development of digital technologies. However, effective tools to accelerate the verification are rare as the process takes time. This study provides a prototype of the UniverCert platform based on a consortium version of the decentralized, open-source Ethereum blockchain technology. The proposed platform is based on a globally distributed peer-to-peer network that allows educational institutions to partner with the blockchain network, track student data, verify academic performance, and share documents with other stakeholders. The UniverCert platform was developed on a consortium blockchain architecture to address the problems universities face in storing and securing student data. The system provides a solution to facilitate students' registration, verification, and authenticity of educational documents.

Keywords: Blockchain, smart contract, academic records, verification.

1 Introduction

One of the most important issues in the field of education is the safe storage of student/graduate academic performance and its supporting documents (diploma, transcript etc.), as well as quick and easy access to the accuracy of this information. In most cases, the official documents (diploma,

certificate etc.) which confirms the student's graduation contains the following information such as course number, course title, the letter grades, and GPA (grade point average), accordingly, detailed information on the student's academic performance for a certain period (semester) or for throughout academic years in higher education institution will not be available. This issue not only worries the institutions but also the students/graduates, state organs, law enforcement, as well as employers.

With the recent development of the Internet and digital technologies in the education system, the process of verifying the authenticity of digital documents issued by higher institutions has become a pressing issue. As few tools are available to verify the authenticity of official documents. Yearly, approximately 500 thousand cases of university diploma authentication are registered in the Republic of Kazakhstan. This process takes time, as the copies of the documents are stored in the university file. Similar problems are noted in higher education systems globally. According to UNESCO 30% of senior managers work with fake qualifications globally [6]. In addition, the process is lengthy and inconvenient as graduates must contact the university to obtain replacement education documents in case of loss, with these shortcomings, companies face daunting tasks to verify documents.

Many higher education institutions (HEIs) develop digital versions of educational documents (university diplomas, diploma supplements, academic transcripts, certificate of non-formal education) in their Learning Management System (LMS) systems, which employees can access. In addition, students can view or print out their academic records using a restricted, password-protected mode. However, the databases are located in a single location and vulnerable to unauthorized access [7].

According to the internal policies of the document management system, universities not authorized to transfer students' data to third parties. Thus, students who transfer to another university may obliged to confirm the authenticity of their documents. Organizing external academic students is the main problem because language, writing, and administration are the major barriers. Moreover, these records are stored using different standards, hindering the exchange of academic records between universities [20].

Thus, creating digital tools is crucial to forming a trust base integrating educational documents, preventing stored data from falsification, and document verification and authenticity. These problems are solved using the basic principles of blockchain technology.

Based on the above, we will determine the main problem of guaranteeing the security and authenticity of digital documents in the education system: the lack of a description of the mechanism for verifying students' documents and their academic history of academic performance and presentation to interested parties.

The purpose of the study is to develop a software product that allows verification of documents with minimal time spent on requests and data processing, with a high level of information security and providing it depending on the level of user access.

This study proposes a web platform developed by UniverCert using an Ethereum consortium blockchain architecture to store the academic records of students/graduates, develop future digital educational documents, and provide third-party document verification services.

The UniverCert platform is based on blockchain technology using an immutable distributed data storage system to store the academic records in a secure information system [11] and form a trusted digital register of educational documents. Moreover, the applied Ethereum solution helps build the logic of the transaction through smart contracts to manage data storage and retrieval. The platform allows universities to create an effective, and convenient global environment.

This study provides several contributions:

- First, the study provides a comparative analysis of related studies on blockchain technology in higher education;
- Second, we identify and justify an acceptable and open source blockchain, platform to solve the research problems;
- Third, we describe a mechanism for verifying the authenticity of data in the blockchain network, depending on the level of access and provision of information to interested parties;
- Fourth, we design and discuss the architecture that interacts with different systems and databases.

The rest of the paper is organized as follows. Section 2 explores the related studies. Section 3 provides the background of the blockchain platform. Section 4 presents the results and discussion. Finally, Section 5 concludes the paper.

2 Related work

Blockchain technology is a distributed network [13] to store a block data structure [15] through cryptographic processing [5], using transaction coordination algorithms [14] in the network nodes. Blockchains store data using innovative software and sophisticated math rules, which are extremely difficult for attackers to fake. The development of cloud services helps higher institutions to develop digital versions of educational documents using blockchain technologies. In addition, blockchain technology offers a unique tool to protect and authenticate official university documents.

At present, many higher institutions have developed different approaches to store and verify academic documents using blockchain technologies. The goal is to facilitate documents' authenticity and reliability, thereby adhering to the principles of decentralization, transparency, and confidentiality. Table 1 summarizes the parameters of blockchain approaches adopted by different institutions

- Reasonable choice blockchain classification to tackle assigned tasks,
- Covering stakeholder interests,
- Availability of verification process.

With blockchain technology the Massachusetts Institute of Technology (MIT) [32] has implemented an effective framework to protect and confirm the validity of diplomas and certificates. MIT has released several versions of the Blockcerts program [19], to issue certificates Since 2018, the MIT University has offered students the opportunity to receive a digital version of their diplomas through the blockchain as part of a pilot program to secure academic data and facilitate their portability. The system standardizes the issuance of diplomas and stores them in a single database. Thus, the university uses Bitcoin platform technology to store the hash code of documents on the blockchain network [23].

The University of Nicosia (UNIC) [35] uses a similar MIT program to create and store certificates using the Bitcoin platform. In addition, the university accepts bitcoins as a form of payment to study a degree program. This scenario expensive for platform users, as it involves storing big data and documents like diplomas, certificates, and transcripts.

A study identifies EduCTX to describe a blockchain-based decentralized credit platform for higher education, using the principles and rules of the European Credit Transfer and Accumulation System (ECTS) [22]. EduCTX offers a comprehensive and unified digital environment designed according to the following scenarios: management, assignment, and presentation of digital micro-credentials [9]. In the proposed solution, students' academic performance is treated as ECTX tokens. After the students successfully pass the exams, the professors check the results, and the administrative office transfers the corresponding credits to the student's wallet and the central blockchain network. The proposed solution is aimed at replacing the traditional assessment system with a digital assessment system using a distributed peer-to-peer (P2P) network. While the new technology provides students the tools to manage their academic credits, the solution is devoid of the verification process.

The Sony Corporation and Sony Global Education is also use blockchain technology for certification training systems [34]. The technology is based on the centralized data management system that many educational organizations use to record and identify official educational data and digital transcripts. The Sony Corporation also uses a new service (Education Blockchain) manage official transcripts and grade academic records through a digital platform. Since no detailed information about the technology is provided, the system appears to store and secure the official academic records.

The Financial University in Moscow, Russia has launched a blockchain-based service to verify academic records on its official website [33]. The university offers a platform where students enter their data and diploma information, then send a request to obtain a hash diploma. The service

is only for students at the university and not for other stakeholders in the university. Moreover, the service does not take into account the interests of stakeholders attempting to verify students' academic information.

The BlockFactory in Switzerland developed CertificationIO [31], which uses the Ethereum blockchain to obtain a hash result of the electronic version of the education document. With the hash result, the document is transformed using an electronic digital signature and provides the user a ready-made signature. To store data through the hash result, the General Data Protection Regulation must be followed [18] to save resources when processing a transaction in a public blockchain network. LMS systems have been integrated into the API channel of universities and services of recruiting agencies. However, CertificationIO cannot store the student's progress record for the entire study period. Consequently, the system cannot form a complete picture of a student's progress and cannot regenerate digital versions of documents.

SmartCert is another blockchain-based digital credential verification platform developed to authenticate academic credentials for Al-Zaytoonah University of Jordan [10]. SmartCert uses cryptographic signatures for the security of educational certificates. Thus, the system is useful for students and universities as it facilitates certificate verification with the prospective employer. However, a third party can attack the computer system and access protected data if in possession of a hash or digital signature. As a result, access to the legitimate user is restricted.

Table 1 provides a comparative analysis of related works.

Table 1: Comparison of blockchain technologies of educational institutions

Institutions/ approach	Decentralized	Transparency	Privacy	Blockchain type	Coverage of stakeholders	Availability of verification process	Data source
MIT	+	+	-	public	- institutions, - graduates	need improvements for the authenticity of the third party	https://www.blockcerts.org/
UNIC	+	+	-	public	- institutions, - graduates, - employer	need improvements for employer verification	https://block.co/
EduCTX	+	not completely fulfilled	+	Consortium	- institutions, - students/ graduates, - employers	not available	https://eductx.org/
Education Blockchain	+	+	+	consortium	- institutions, - students	not available	https://blockchain.sonyged.com/
The Financial University of Moscow	+	not completely fulfilled	+	private	- institutions, - graduates	not available	http://www.fa.ru/
CertificationIO	+	not completely fulfilled	not completely fulfilled	public	- institutions, - students/ graduates, - employers	verification of the authenticity of the EDS within the document	https://certifaction.io/
SmartCert	+	not completely fulfilled	+	consortium	- institutions, - students/ graduates, - employers	no specific information	https://www.zuj.edu.jo/
UniverCert	+	not completely fulfilled	+	consortium	- institutions, - students/ graduates, - state organs, - law enforcement, - employers	provided a clear verification algorithm for each stakeholder based on access levels	under development

Table 1 reveals various technologies aimed at storing secured ready-made educational documents (certificates, diplomas) and compares the key principles of the technologies such as decentralization, transparency, and confidentiality. However, some of these technologies do not provide academic ver-

ification services, the technologies are not aimed at storing the history of academic performance and other similar data of students/graduates in digital versions. Thus, novel technology is critical to store and secure education documents. The transition of education documents into digital versions using a decentralization approach will enhance a student's progress.

This study proposes a prototype of the UniverCert based on the decentralized, open-source Ethereum blockchain platform to store and secure education documents.

3 Background

The proposed UniverCert platform is an advanced digital service information system for educational institutions. The platform is designed to modernize existing LMS systems to store university data. The aims of UniverCert platform are:

- to consider the available technological tools (for example, KazNU has LMS Univer 2.0, OpenKazNU).
- to justify the choice of blockchain technology (the Ethereum platform and smart contracts).
- to consider the types of blockchain and digital certificates for authentication.

3.1 Information system Univer 2.0

The benefit of the UniverCert platform is its direct integration with the university's LMS system, which forms data from official education documents. The information system "UNIVER 2.0" is an example of an automated information system used by al-Farabi Kazakh National University. The "UNIVER 2.0" offers the digital transformation of the university business processes, storing data related to the applicant's enrollment and educational documents. However, the system fails to provide a decentralized storage platform to verify the educational documents. The implementation of direct LMS integration and the decentralized platform at the RestAPI level will optimize and protect the documents from modification. Moreover, the system facilitates document approval and storage to reflect the information of student qualification and academic performance.

3.2 OpenKazNU

Rapid development in Internet technology and digitalization has motivated many universities to introduce online learning at various sites in Kazakhstan (e.g., moocs.kz, open.kaznu.kz, dl.kaznu.kz). Kazakhstan recognizes the results of non-formal learning and includes the course credits in the student's transcript. The mechanisms for recognizing massive open online courses (MOOC) allow MOOC's students to convert into enrolling in a traditional learning [Validation of Non-formal MOOC-based Learning] process. For example, through the activities of Knowledge Media Institute (KMi) of Open University, research and development have successfully been implemented through an online learning process. KMi has participated in many research initiatives using the blockchain. Open University is a leader in UK distance education, and it provides KMi the opportunity to badge all Open University courses and notarize them on the blockchain.

3.3 Ethereum and Smart Contracts

The Ethereum solution was chosen to create the UniverCert platform. Ethereum has many important features that distinguish it from other systems [1, 4]. Table 2 shows the key aspects of different blockchain platforms.

The Ethereum platform allows developers to create any system based on the blockchain functions, using smart contracts to automatically perform actions. Ethereum was chosen as a suitable platform, taking into account several features, such as high transaction speed per second, a large selection of programming languages, and support of smart contracts.

A smart contract is a digital contract written in source code and executed by computers that integrates a blockchain security mechanism against unauthorized access [12]. Smart contracts are

Table 2: Comparison of key aspects of different blockchain-based platforms

No	Platform	Average performance, TPS	Scalability, TPS	Consensus	Smart contracts	Development languages	Encryption	API	Data source
1	Bitcoin Green	154	-	The Green Protocol	-	C++, JavaScript, Python	No data	-	https://bitcoin.org/
2	Ethereum	15	5000	Proof-of-Work	+	C++, Go, Rust, Solidity, Serpent	ECDSA	+	https://ethereum.org/
3	Ripple	1500	70000	Ripple Protocol consensus algorithm	+	Solidity, Serpent	GOST R 34.10-2001	+	https://ripple.com/
4	R3 Corda	170-250	-	Raft Algorithm /Byzantine Consensus	+	Java, Kotlin	ECDSA/RSA	-	https://www.corda.net/
5	Hyperledger Fabric	200	1350	PBFT, PoET1	+	Go, Java	ECDSA	+	https://www.hyperledger.org/

developed using the Solidity programming language [17]. The code written in Solidity is compiled and converted to bytecode and sent to the Ethereum blockchain as a smart contract. Smart contracts and blockchain applications are running on an Ethereum Virtual Machine. Smart contracts, using predefined conditions built into the algorithm, facilitate document verification without human intervention.

3.4 Blockchain types

Before choosing a blockchain platform, it is crucial to understand the blockchain suitability for a particular use case. Three main types of blockchain are as follows:

1) A public blockchain has a ledger visible to everyone on the Internet, which allows the public to check and add a block of transactions to the blockchain [26]. Identity verification is not required on a public blockchain, showing that privacy is not guaranteed. Thus, it is unprofitable for universities, students, and third parties to connect to public blockchain networks, as they incur financial costs to store data or make transactions [25].

2) A private blockchain is a distributed yet centralized network that permits few people in an organization to check and add blocks of transactions. However, all Internet users are allowed to view the ledger [3].

3) The consortium blockchain uses network nodes, where multiple organizations engage in transactions [27]. A consortium blockchain is a mixture of the two previous types, with only privileged participants performing operations in the consensus process.

The UniverCert system has chosen a consortium blockchain. For decentralized structures and self-regulating consortium blockchain networks, the participating nodes must agree with the current state of the ledger content. This is a technique to pack unconfirmed data into blocks and add them to the ledger.

In addition, we chose the Proof-of-Work (PoW) algorithm as the distributed consensus algorithm to support the network state [16, 28, 29]. However, PoW-based blockchain requires considerable computing power and energy consumption. At the same time, PoW is one of the most common consensus algorithms, effective for preventing denial of service and distributed denial of service attacks

on the blockchain.

3.5 Blockchain-based digital certificates

A certificate is a unique, signed document issued by one party to authoritatively identify an individual's identity. In the field of education, the certificate confirms the achievement of learning outcomes, completion of a certain stage of training, level of qualification, or total credits in non-formal education. Certification is a procedure for issuing a certificate and verifying the document by a third party. Educational certificates were issued to students who graduated from universities or other institutions. Certificates also offer opportunities for graduates to further their studies, gain employment, and verify their data. Digital certificates based on blockchain technology have many advantages: certificates cannot be forged as they accurately indicate the party that issues and the party that receives the certificate. Verification can be performed by a member of the consortium who has access to the blockchain. You can obtain a certificate confirmation from an organization that no longer exists or has changed its name. In this case, the blockchains can store either cryptographic hashes of certificates or the certificates themselves.

Organizations provide professional training for a future employee as it is not enough for employers to have only an education diploma, which contains the university name, the full name of the recipient, the issue date, and degree awarded. This information is stored as text in the blockchain to create a degree-awarding database. As a certificate hash, the goal is to protect an issued digital certificate.

With blockchain solutions for higher education, only diplomas and diploma appendices are presented as documents for validation. The proposed UniverCert system will store the following digital certificates:

- Diploma of education (a document on the completion of the bachelor's, master's, or doctoral degree level);
- An academic transcript, which details the student's academic performance history;
- Diploma supplements in three languages: Kazakh, Russian, and English (diploma supplement);
- Certificates of completion of MOOCs with credit transfer.

4 Findings and discussion

This section describes a comprehensive solution designed to track and release academic records of students/graduates by (1) choosing the appropriate type of data storage, (2) describing the system architecture, and (3) describing smart contracts.

4.1 Proposed solution

The proposed UniverCert platform was built using the Ethereum blockchain platform and deployed as a P2P network consortium architecture [8]. Higher education institutions are the peers of the blockchain network, and the users of the platform are organizations (e.g., governments, law enforcement agencies, and employers).

The blockchain platform with a consortium architecture has the following differences:

- Regulatory participation and governance. Many studies suggest that benefits derived from its regulations are suitable for the educational system [2, 21, 24, 30]. Flexible rules of the consortium coordinate the actions of all network participants;
- Role-based access mechanism. The ability to assign roles according to the needs of stakeholders. Access levels are adjusted according to the requirements for personal students' security or security of educational information;
- Target audiences. The stakeholders are much broader than that of other types of blockchain.

4.2 System architecture

Figure 1 shows the entire process of tracking and issuing academic documents, which include processing Off-chain data and processing On-chain data. Given the diversity of the university LMS systems in terms of the stored data structure and functionality, it is advisable to offer a RestAPI solution as a universal technology to integrate the university system and blockchain exchange platform.

Interaction via RestAPI

RestAPI (representational state transfer) - access to the blockchain platform is carried out through the RestAPI channel. The RestAPI uses ready-made methods to store data and search data using several filters (student ID, university ID). These methods are available to organizations based on their access levels. The RestAPI is extended with new methods to connect third-party organizations (employers, government agencies), which is one of the advantages of the proposed solution.

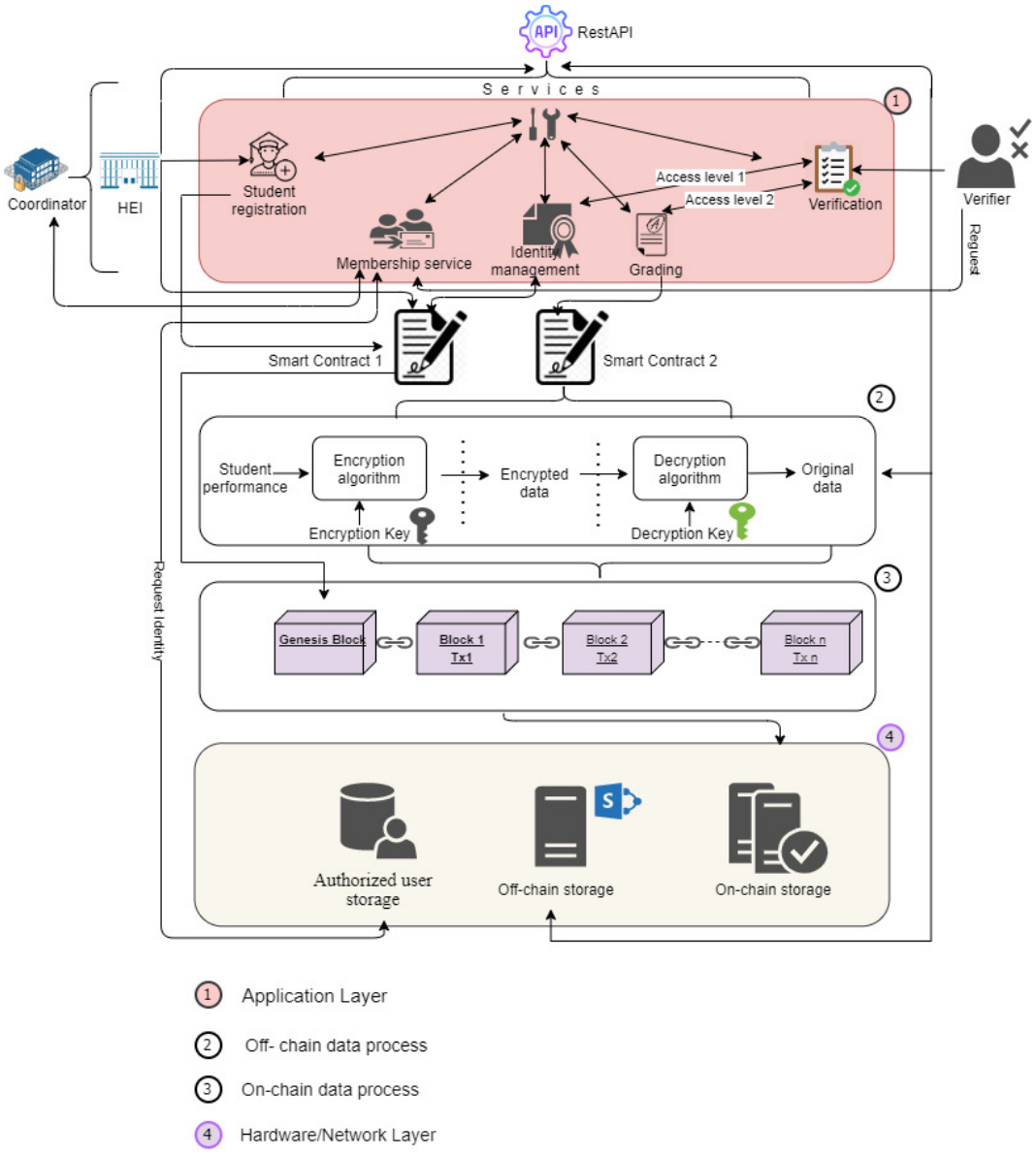


Figure 1: Architecture of the proposed platform

1. Application Layer

At the top of Figure 1, user interfaces for organizing services are student/graduate registration, organization registration, assessment, and verification. Below is a more detailed description of each service.

- Student registration

The university enters the student's data in the LMS system and issues a unique student ID following the enrollment number. This data is obtained through the ID. This data is unencrypted and stored in its original form in the blocks of the blockchain network as a genesis block. To store the above data, a single Smart Contact-1 is used, which is described in detail below.

- Membership service

Organizations (government, law enforcement, educational institutions) that want to connect to the platform contact the network coordinator to access information about a student/graduate.

- Grading system

After a semester, the university uses a grading system to assign grades for all courses and transfer them to the blockchain platform.

- Verification

In the education system, blockchain technology does not offer the verification process or a clear verification method, which is a key for confidentiality. Our verification process is formulated as follows:

I. Any interested party (government agency, employer) must first obtain authorized access to the platform.

II. According to the request for authorized access, the Platform coordinator issues an API key to connect the RestAPI and obtain the necessary data.

III. The entire verification process is divided into two levels, depending on the needs of the organizations. Access level 1 – verifying the authenticity of academic records of students/graduates using Smart Contract-1. Access level 2 – obtaining detailed information about the academic achievements of students/graduates using Smart Contract-2 and a key pair (university and student ID).

2. Off-chain data process

After the semester examination, the student's grades are stored in the system with the support of various smart contracts (1, 2), described in more detail in subsection 4.3.

After the Smart Contact-2 rule is executed, the next data processing starts outside the network:

- The symmetric encryption offers security for student/graduate performance data.
- The decryption process is a procedure for decrypting student/graduate performance data.

The second level of access enhances the confidentiality of critical academic data.

3. On-chain data process

This process starts with the generation of "Genesis Block" or the first block for the student. Then, all transactions are recorded in the blockchain. Each block contains a unique header, identified by its block header hash. The block consists of three main components: a previous block hash, data (specialties, discipline, and score), and timestamp. This process is repeated each semester until the students graduate from the University.

4. Hardware / Network Layer

As illustrated in Figure 1, the hardware layer consists of three components: authorized users storage, Off-Chain data storage, and On-Chain data storage.

- Authorized users storage – a centralized database of an organization (government agencies, employers) registered as users. It uses a membership service that has access to retrieve data using RestAPI.
- Off-chain data storage – a centralized database of directories (specialties, disciplines).

- On-chain data storage – a consortium blockchain that operates under the leadership of a group of entities, enabling collaborative business transformation among organizations. In our case, the coordinator assigns unique access for each user (state organs, employer).

Verifier

The verifier is any organization who has the right to view and verify the validity of academic records. The client-side verification process is carried out in two ways: a verifier wants to authenticate the identity of student/graduate official records (level 1) or may additionally request access to receive detailed information (level 2). Only the verifier can view unverified documents to enhance confidentiality.

HEI (higher education institution)

The proposed system optimizes the university business processes as it stores and secures student data. When a student is transferred to another university that connects to the network, the system provides the flexibility of exchanging learning outcomes among educational institutions. Thus, it prevents costs associated with the processing times, manual work, postal fees, and transit. The benefits are as follows:

- A collaborative environment between different institutions will be available, eliminating challenges of the education system, thereby improving the quality of education.
- The system will keep the academic record unchanged and share it with all authorized organizations.

Coordinator

Our proposed platform is adapted to a consortium blockchain network. Moreover, a consortium blockchain works under the governance of the coordinator. In our proposed architecture, the coordinator can become the administrator of the entire system and the main node in the network according to its associated privileges. For the coordinator, this is an indispensable tool to track the activities of higher education institutions:

- The coordinator can control the quality of the services that the university offers to students, thereby preventing fraudulent activities.
- The coordinator can create a unified digital register of student/graduate official academic documents stored on the blockchain network by generating electronic versions of documents such as diplomas, diploma supplements, and transcripts with the digitally signed platform. With the system, printing academic records are not required.
- The coordinator can eliminate the possible costs associated with the centralized approach like processing times, manual work, postal fees, and transfer processes.

To describe the system with all its entities, and how it processes as a whole, in Fig.1 has been included with a brief description about obtaining information processes and about all its input, output data.

- Obtaining open information about the student/graduate and the university. The interested party makes a request and receives the following data: student, university, when he/she entered and graduated, specialty, qualification. These data are not encrypted in the blockchain platform, as they do not carry confidential information. This data allows the interested party to make sure that the graduate/student really studied at the specified university.
- Getting the student/graduate academic performance history. This is the second level of access. The administrator-the organization, according to the request of the interested party, provides this access. The interested party (state agency, university, graduate) makes a request and receives the following data: Student, Discipline, Academic performance (credit, grade). This

data is encrypted with symmetric encryption based on the key (student ID and university ID) to maintain data confidentiality. This data is needed so that the interested party can see the true history of the student's/graduate's academic performance.

- Obtaining the rights to store data. This access is provided to universities and other educational organizations in order to they can fill the blockchain platform with data about students (students, graduates, etc.).

4.3 The usage of smart contracts

In our proposal, we developed two smart contracts as basic elements of the blockchain technology, which are a set of rules that allows organizing different levels to access data (Figure 2 and Table 3).

Table 3: Smart contracts

Smart contracts	Description
Smart Contract-1	Store student personal data
Smart Contract-2	Store data about the student's performance

Figure 2 illustrates the smart contract sequence diagram −1.

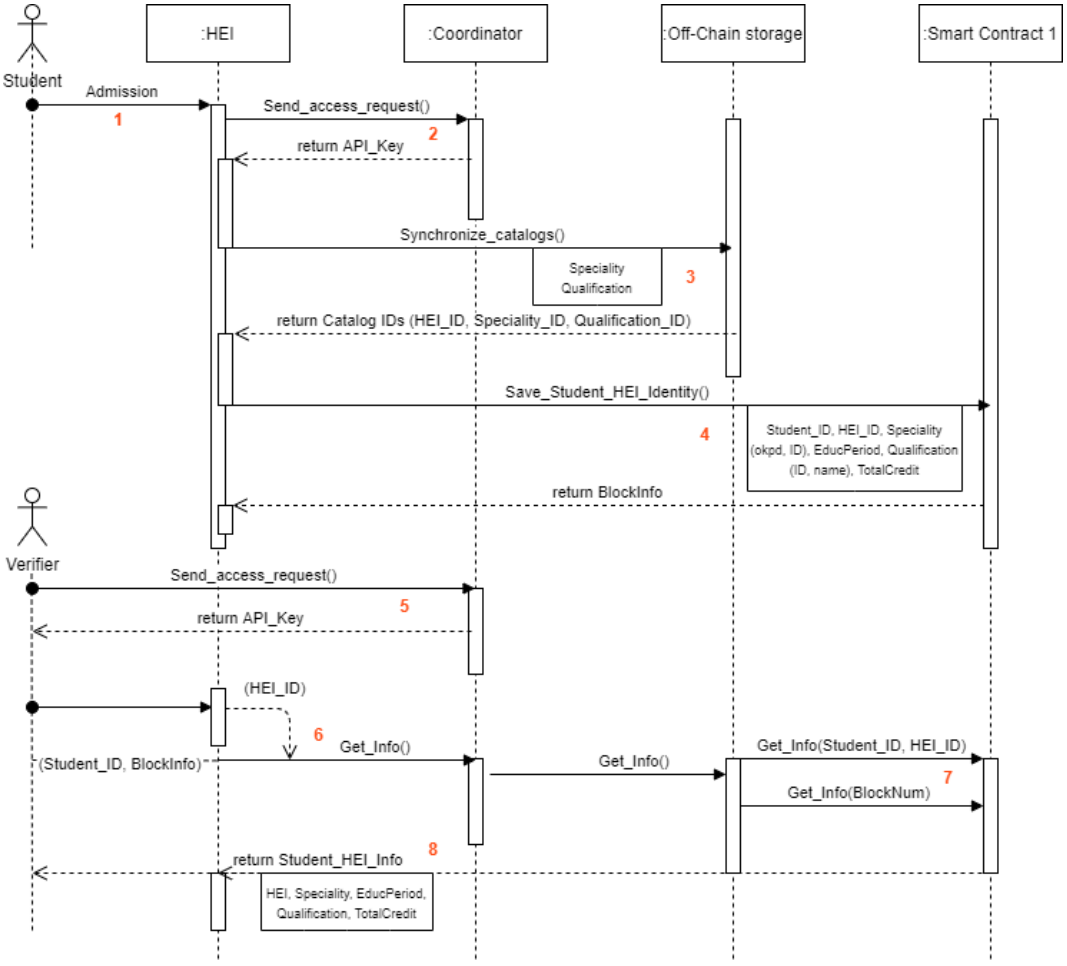


Figure 2: Sequence diagram of Smart Contract-1

Smart contract-1 stores the following data: university, specialty, year of admission and graduation, level of study, and academic degree. The data is not encrypted, and it is stored in the blockchain network blocks. The student data are obtained by the student ID without additional access. The interaction between the system is described below:

1. Student enrollment in the LMS system. The student is enrolled and provides specialty of training conditions: the study period, total number of credits, and qualifications after graduation.

2. Access the student's academic data. Access rights are granted by the platform coordinator. Access rights are the process of an API key to work with RestAPI.

3. When a university is registered in the platform, all reference data (specialties, qualifications, catalog of disciplines) are synchronized with the central repository of the coordinator. The Off-Chain storage keeps all connected universities specialties (specialty names in three languages, code, requirements, and qualifications). To save memory, specialty identifiers and qualifications are stored in blocks instead of names.

4. The process of registering a student in the blockchain platform is carried out by linking the student to the university specialty. Thus, the university receives a unique block address and stores it in the LMS system.

5. An organization that wants to verify the accuracy of the student's information should connect to RestAPI. To achieve this objective, the coordinator must provide the appropriate access (access level 1) and API key.

6. An organization that intends to validate the data makes a request to the platform using the student ID. The identifier is provided by the student or graduates. In addition, the student can provide the university identifier, saved in the QR code of the diploma or transcript.

7. Three methods are implemented at the Smart contract 1: search by student ID, search by student ID and university ID, as well as search by block address. All three methods provide student information and specialties

In Figure 3, the sequence of operations of Smart contract-2 includes processes (data encryption and decryption) and an additional component (Smart contract 2), in addition to the components Smart contract-1.

Smart Contract 2 handles student/graduate achievements. The interactions between the system's components are indicated by numbers, as described below:

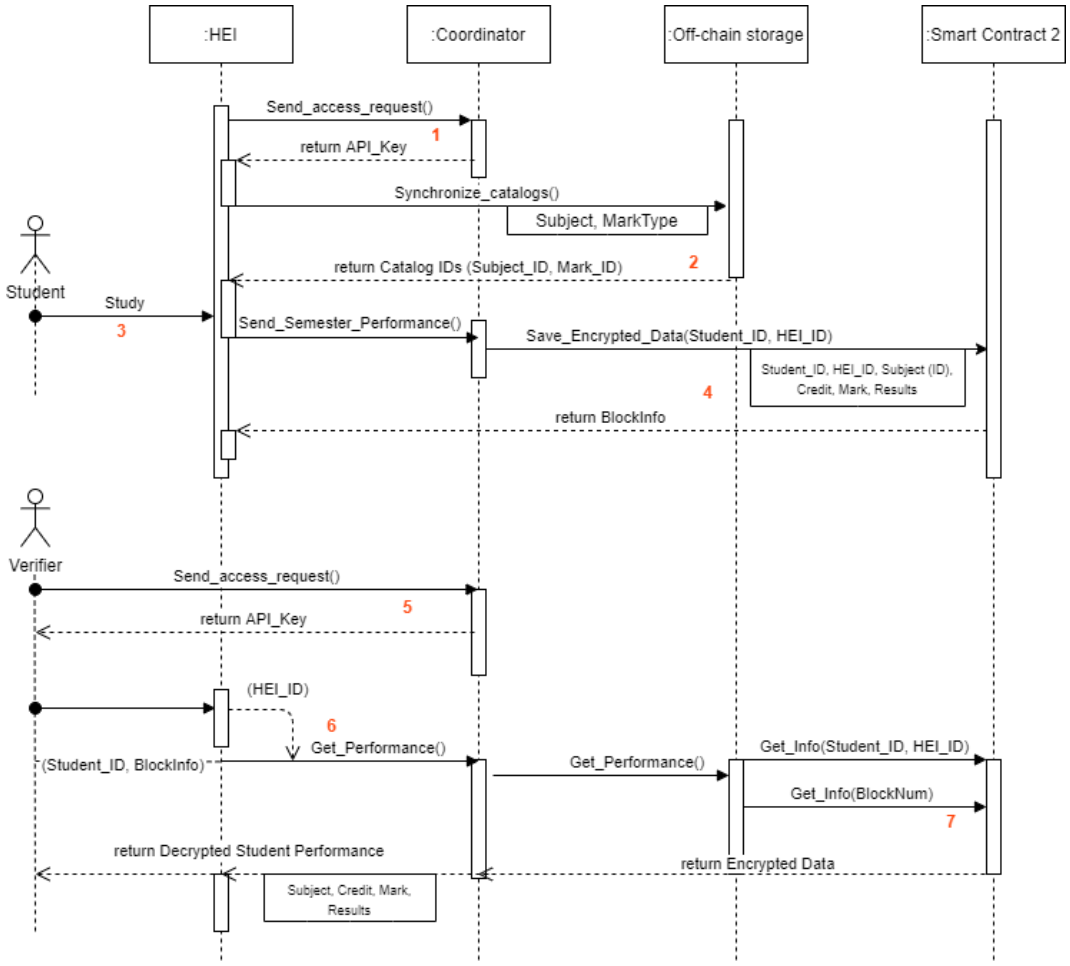


Figure 3: Sequence diagram of Smart Contract-2

1. The process of a university to gain access to the student performance data.

2. The process of synchronizing the catalog of disciplines and types of grades with the central storage (Off-chain storage). All disciplines with a full description (in 3 languages, qualification obtained after completing the course) and assessment types (all types of assessment) must be synchronized with the coordinator's database. In the future, the discipline ID and the scores to be stored in the blockchain are taken from storage to save memory and optimize transaction processing.

3. The process of student learning. At the end of each semester, the student receives a final grade for each course.

4. The process of transferring the completed courses to the blockchain database. The University's LMS system connects to the RestAPI platform via an API key and transmits information in a specific format. At the coordinator level (inside the RestAPI service), symmetric data encryption takes place (the key is the student ID and the university). Only encrypted information is transmitted to the blockchain database, except the student and university ID to facilitate its accessibility in the future. Smart contract 2 returns the unique address of the block where the information is stored. The block address will be saved in the university's LMS system, and the university can use it to generate a QR code digital versions of the transcript, diploma supplement), as well as to obtain encrypted information from Smart Contract 2 using the block number.

5. To allow the university to have access to the student's academic data in the platform, access rights are granted by the platform coordinator. Access rights are used to obtain an API key to work with RestAPI.

6. The process of accessing the platform via RestAPI to obtain confidential information, in which an API key, student, and university IDs are transmitted.

7. Smart Contract 2 returns encrypted information. At the RestAPI level, the information is decrypted using a key (student and university ID).

5 Conclusion and future research

The problem of verifying the authenticity of documents on the education of graduates and the academic performance of students was not effectively solved. Blockchain technology allows you to solve this problem.

In the process of working on the problem:

- we have identified and discussed blockchains and their main functions;
- conducted a comparative analysis of research on blockchain technology in higher education;
- presented a mechanism for verifying data in the blockchain network, depending on the level of access and provision of information to interested parties;
- we have developed a consortium architecture of the UniverCert platform, which interacts with various systems and databases.

This study designed a novel platform UniverCert to track academic performance, issue educational certificates, and protect data from forgery. This solution shows the entire process (Off-chain and On-Chain) that includes a student's registration, verification, and authenticity of educational documents. The platform facilitates credit transfer from one university to another and provides a flexible service for checking a student's progress. For future work, we will deploy the proposed platform for many higher educational institutions.

6 Acknowledgment

This work was funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan [Grant No. AP08857535-OT-20]. Development and Implementation of Information System for document verification in Higher education (universities) of Kazakhstan which is integrated into the international platform.

References

[1] Aung, Y.N. (2017). Review of Ethereum: Smart Home Case Study, *2nd International Conference on Information Technology (INCIT)*, 2017.

[2] Cai, W.; Wang, Z., Ernst, J.B., Hong, Z., Feng, C., Leung, V.C.M. (2018). Decentralized applications: The blockchain-empowered software system, *IEEE Access*, 6, 53019–53033, 2018.

[3] Dinh, T.T.A.; Wang, J., Chen, G., Liu, R., Ooi, B.C., Tan, K.L. (2017). Blockbench: a framework for analyzing private blockchains, *International Conference on Management of Data*, 1085–1100, 2017.

[4] Eduardo de Azevedo Sousa, J.; Oliveira, V., Valadares, J., Gonçalves, G.D., Villela, S.M., Bernardino, H.S., Vieira, A.B. (2020). An analysis of the fees and pending time correlation in Ethereum, *International journal of Network Management*, 31(3), 2020.

[5] Fernández-Caramés, M.T.; Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks, *IEEE Access*, 21091–21116, 2020.

[6] Grolleau, G.; Lakhal, T., Mzoughi, N. (2008). An introduction to the Economics of Fake Degrees, *Journal of Economic Issues*, 42(3), 673–693, 2008.

[7] Han, M.; Li, L., Xie, Y., Wang, J., Duan, Zh., Li, J., and Yan, M. (2018). Cognitive approach for location privacy protection, *IEEE Access,* 6, 13466–13477, 2018.

[8] Kamišalić, A.; Turkanović, M., Heričko, M. (2018). A decentralized system for managing micro-credentials based on blockchain 2.0, *10th International Workshop on Data Analysis Methods for Software Systems*, 39, 2018.

[9] Kamišalić, A.; Turkanović, M., Mrdovi, S., Heričko, M. (2019). A Preliminary Review of Blockchain-Based Solutions in Higher Education, *Springer International Publishing*, 114–124, 2019.

[10] Kanan, T.; Obaidat, A.T., Al-Lahham, M. (2019). SmartCert BlockChain Imperative for Educational Certificates, *IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 629–633, 2019.

[11] Li, M.; Tang, M. (2013). Information Security Engineering: a Framework for Research and Practices, *International Journal of Computers Communications & Control*, 8(4), 578–587, 2013.

[12] Lin, X. (2017). Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the Ethereum Blockchain, *Taiwan, R.O.C.*, 2017.

[13] Liu, D.; Ni, J., Huang, C., Lin, X., Shen, X. (2020). Secure and Efficient Distributed Network Provenance for IoT: A Blockchain-based Approach, *IEEE Internet of Things Journal*, 7(8), 7564–7574, 2020.

[14] Mingxiao, D.; Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C. (2017). A Review on Consensus Algorithm of Blockchain, *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2017.

[15] Monrat, A.A.; Schel'en, O., Andersson, K. (2019). A Survey of Blockchain from the Perspectives of Applications, Challenges and Opportunities, *IEEE Access*, 117134–117151, 2019.

[16] Nakamoto, S. (2018). Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

[17] Patel, D.; Bothra, J., Patel, V. (2017). Blockchain exhumed, *ISEA Asia Security and Privacy (ISEASP)*, 1–12, 2017.

[18] Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR), *Human Genetics*, 575–582, 2018.

[19] Santos, J.; Dufy, K.H. (2018). A Decentralized Approach to Blockcerts Credential Revocation, *A White Paper from Rebooting the Web of Trust V*, 2018.

[20] Selingo, J. (2017). The future of the degree: How colleges can survive the new credential economy, *The Chronicle of Higher Education*, 2017.

[21] Shen, H.; Xiao, Y. (2018). Research on Online Quiz Scheme Based on Double-layer Consortium Blockchain, *9th International Conference on Information Technology in Medicine and Education*, 2018.

[22] Turkanović, M.; Hölbl, M., Košič, K., Heričko, M., Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform, *IEEE Access*, 5112–5127, 2018.

[23] Vujičić, D.; Jagodić, D., Ranđić, S. (2018). Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview, *IEEE 17th International Symposium INFOTECH-JAHORINA*, 2018.

[24] Wang, G.; Zhang, H., Xiao, B., Chung, Y., Cai, W. (2019). EduBloud: A Blockchain-based Education Cloud, *Computing, Communications, and IoT Applications (ComComAp)*, 2019.

[25] Xiao, Y.; Zhang, N., Lou, W., Hou, Y.T. (2020). A Survey of Distributed Consensus Protocols for Blockchain Networks, *IEEE Communications Surveys & Tutorials*, 1432–1465, 2020.

[26] Xu, L.; Shah, N., Chen, L., Diallo, N, Gao, Z., Lu, Y., Shi, W. (2017). Enabling the sharing economy: privacy respecting contract based on public blockchain, *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, ACM*, 15–21, 2017.

[27] Yaga, D.; Mell, P., Roby, N., Scarfone, K. (2018). Blockchain Technology Overview, *National Institute of Standards and Technology Internal Report*, 2018.

[28] Yli-Huumo, J.; Ko, D., Choi, S., Park, S., Smolander, K. (2016). Where is current research on blockchain technology? *A systematic review, PLoS ONE*, 11(10), 2016.

[29] Zheng, Z.; Xie, S., Dai, H., Chen, X., Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends, *IEEE International Congress on Big Data (BigData Congress)*, 557–564, 2017.

[30] Zhong, B.; Haitao, W., Ding, L., Luo, H., Luo, Y., Pan, X. (2020). Hyperledger fabric-based consortium blockchain for construction quality information management, *Frontiers of Engineering Management*, 7, 512–527, 2020.

[31] [Online]. Certification, Diploma certification for education institutions, https://certifaction.io/diploma-certificatio/

[32] [Online]. MIT, Digital Academic Credentials, https://www.media.mit.edu/projects/media-lab-digital-certificates/overview/

[33] [Online]. Moscow Leningradsky. (2018). Graduate Diploma Verification in Blockchain, http://www.fa.ru/checkdiploma_blockchain/Pages/Home.aspx/

[34] [Online]. Sony Global Education. (2019). Sony develops system for authentication, sharing, and rights management using blockchain technology, https://www.sonyged.com/2017/08/10/news/press-blockchain/

[35] [Online]. UNIC. (2018). Blockchain Certificates (Academic & Others), https://www.unic.ac.cy/iff/blockchain-certificates/

Journal's webpage: http://univagora.ro/jour/index.php/ijccc/

This journal is a member of, and subscribes to the principles of,
the Committee on Publication Ethics (COPE).
https://publicationethics.org/members/international-journal-computers-communications-and-control

Cite this paper as:

Shakan, Y.; Kumalakov B.; Mutanov G.;, Mamykova Zh.; Kistaubayev Y. (2021). Verification of University Student and Graduate Data using Blockchain Technology, *International Journal of Computers Communications & Control*, 16(5), 4266, 2021.

https://doi.org/10.15837/ijccc.2021.5.4266