Intellectual property assurance method for digital university ecosystem based on blockchain technology

Oleksandr Kapliienko[a], Galyna Tabunshchyk[a], Tetiana Kapliienko[a] and Carsten Wolff[b]

[a] *National University "Zaporizhzhia Polytechnic", 64, Zhukovsky Street, Zaporizhzhya, 69063, Ukraine*
[b] *Fachhochschule Dortmund, 23, Otto-Hahn-Str., Dortmund, 44227, Germany*

Abstract
In the university digital ecosystem it is very important to have a proper process of collecting, processing and storing the data about students educational results which could confirm the level of the achieved outcomes within their study. In the paper authors provide an analysis of the data which should be stored and existing system which are used for diploma verification. According to the authors' research, the strategy for the digital transformation of the high educational institutes education system should include the modernization of the management of the intellectual property and learning outcomes (competencies and skills). To provide an intellectual property assurance for the students' documents there were chosen blockchain technology. Intellectual property assurance method for digital university ecosystem based on blockchain technology was proposed by the authors.

Keywords 1
Education, Intellectual property, Learning outcomes, Blockchain, Security, Decentralization, eLearning

1. Introduction

The modern high educational institutes (HEIs) should ensure a study process in the relevant professions and specialties according to the demands the labor market. The learning process should be comfortable and based on the principles of academic integrity. The digital university infrastructure should ensure safety and security for staff and students, specially ensure the intellectual property (IP) of the created academic materials, as some if it according to the national law and regulation should be stored from 5 to 10 years [1].

An important feature of the educational system is an implementation of the different learning approaches and standards in different HEI even in one country, which also change year by year. Accordingly, the presence of a diploma in the same specialty from different institutions and / or from different years of graduation does not imply the presence of the same learning outcomes (competencies and skills). It is also necessary to take into account that students could choose alternative disciplines and internships within their study program, or have additional achievements in the learning process.

To support a coherent and understandable system of an individual's lifelong learning there should be stored a sizable amount of data that needs to be saved for the diploma assurance.

There are a lot of requirements which are put forward for this data:

- they must be ordered by the time of creation;
- intellectual property and personal data must be protected from external access;

CMIS-2021: The Fourth International Workshop on Computer Modeling and Intelligent Systems, April 27, 2021, Zaporizhzhia, Ukraine
EMAIL: alexandr.kaplienko@gmail.com (O. Kapliienko); galina.tabunshchik@gmail.com (G. Tabunshchyk); bragina.zntu@gmail.com (T. Kapliienko); carsten.wolff@fh-dortmund.de (C. Wolff)
ORCID: 0000-0003-2080-7875 (O. Kapliienko); 0000-0003-1429-5180 (G. Tabunshchyk); 0000-0001-8192-2397 (T. Kapliienko); 0000-0003-3646-5240 (C. Wolff)

- the data that confirm the acquisition of certain skills and competencies must be located in the public domain;
- the data should be stored decentralized to avoid loss problems;
- the data should be protected against falsifications, for example change protection or adding faking data.

One of the options for meeting these requirements can be the use of blockchain technology, which introduces immutability and trust to the decentralize data. This paper presents an approach for saving education data based on the blockchain for ensuring the safety and reliability of storing information about the entire learning process for each student (from admission stage to graduation with a HEIs diploma).

2. State of the art

The primary reason for storing of the individual academic materials is the need to confirm the level of education by a certain student (for example, bachelor's, master's degree). Until 2012 in Ukraine, such confirmation was the physical presence of a state diploma, formed by the authorized agency. The disadvantages of this approach were the possibility of forgery or loss of the diploma itself or its supplementary.

In 2012 year, the Ukrainian government introduced the Unified State Electronic Database on Education (USEDE), which is an automated system for collecting, registering, processing, storing and protecting educational information [2]. Since that the diploma as a physical object is not the main goal, the main achievement is the record in this database which confirms the presence of a degree of education of a certain level in a certain specialty.

There are many similar systems and databases in the world that mainly pursue 2 goals:

- obtaining data for statistics [3, 4, 5, 6];
- confirmation of the authenticity of educational documents [7, 8, 9].

For example, the "UIS.Stat" is a product of the UNESCO Institute for Statistics (UIS), which is the official and trusted source of internationally-comparable data on education, science, culture and communication [3]. This system is a comprehensive browser for viewing and downloading the most popular education data and indicators, such as [3]:

- mean years of schooling;
- number and rates of international mobile students (inbound and outbound);
- number of students and enrolment rates by level of education;
- graduation ratio from tertiary education;
- out-of-school children, adolescents and youth (number);
- percentage of graduates by field of education (tertiary education);
- educational expenditure by nature of spending in public educational institutions;
- government expenditure on education (amount);
- survival rate by grade for primary education;
- population of the official age / school age population;
- official entrance age and theoretical duration by level of education (years) and etc.

The OECD.stat database [4] have the similar information provided by the Organization for Economic Co-operation and Development (OECD). In this database there are also information about graduation and entry rates, profile of graduates and new entrants, distribution of graduates and entrants by field, and other indicators. The World Bank EdStats (Education Statistics) portal [5] and Global Education [6] extensive data and analysis source for key topics and a "meta-entry" in education with the visualizations and research. These data make it possible to determine the state of education in a particular country by many different indicators, the progress of development of a particular area, but described systems do not have the opportunity to confirm the level of education of a particular graduate or student.

"DiplomaVerify" and "DegreeVerify" (National Student Clearinghouse Verification Services) [7] gives possibility to instantly verify diplomas for high school graduates of USA (549 educational institutions for this moment) and provides online verifications of college degrees and attendance.

“Nuffic” is the National Academic Recognition Information Centre for Holland [8], the goal of which is to allow to find an equivalent Dutch level of diploma from another country.

The [9] is a service of the "Institut National des Sciences Appliquées" (INCA) of Toulouse that allows to authenticated all INSA diplomas using Prooftag. Prooftag is a security seal and electronic tag found on INSA’s diplomas, which contains a unique code that acts as an electronic birth certificate [10].

The need for the presented systems arose due to the presence of progressive and low-cost scanning and printing technologies, which increase the number of fake academic certificates. These systems represent cooperation within a country, organization or institution.

Since document verification is very important to assure that the diploma is official, some organizations have developed and are presenting their approaches to this systematic process. For example, Documentorum is a global initiative and a new approach to the issuance, registration and verification of certificates and diplomas [11]. It was developed using Hyperledger technology (an open-source collaboration created to advance cross-industry blockchain technologies). It allows students to collect all of their academic data in one place, where it is protected from theft and fraud [11]. Each issued document is automatically verified and approved by the relevant parties and is permanently stored in a tamper-proof ledger on the blockchain, so its authenticity can be always guaranteed.

As we see, most of these systems are oriented on the verification of documents and certificates, which were issued by HEIs and other education organizations, and information about these organizations (formal and statistical). But there is lack of information how HEIs could record information about the learning process that leads to the diploma obtaining. As we mention above, to confirm learning outcomes, competencies and skills of each student, HEI should take into account a lot of information, which must be trustable and with the highest degree of protection against counterfeiting.

For example, storing academic information in learning management systems (LMS) like Moodle does not guarantee that there is no threat of data loss. Conversely, the exclusion of the users who successfully passed the course or training leads to data removal in the system. And even if all information is archived, there is no guarantee of the reliability of the data due to the fact that the system administrator has full access to all data and can change it on the demand.

Since the method of storing data in the blockchain is devoid of these disadvantages, let's look at examples of blockchain technology implementation in the education applications.

There are a number of ways for blockchain implementation in the education field, such as full record of learning trajectory, trusted certification of learning results, decentralized sharing of education resources, etc. The greatest advantage of this network is a decentralized peer-to-peer infrastructure, supporting trust, accountability, transparency, identity management and openness.

In [12] a case study on the decentralization of lifelong learning using blockchain technology was explored. In this case study, the Semantic Blockchain was used as a solution to combine all acquired learning and accreditation experiences to form a holistic picture of a person's lifelong learning. The purpose of this study is to offer transparent and permanent educational accreditation for learners throughout their lives and to support them in their personal and professional progress.

In [13] blockchain technology was used to increase the flexibility of organization the student activity and the results obtained via managing the attendance and the grades obtained by students.

Article [14] describes the problems of online education such as lack of results certification, poor confidentiality and lack of an exchange mechanism. The authors combine blockchain technology with online learning to address these challenges, creating a smart, decentralized and shared online education system.

The article [15] describes research experiments on Smart Pedagogy with a lifelong learning transcript called the passport of knowledge in blockchain architecture. The proposed scenario allows students to publish proof of their academic achievement in blockchain-related formats for instant authentication. The paper describes the experimental network, which consists of three nodes (located in Latvia, in the USA and in Asia). Based on the proposed implementation, this approach validates training evidence much better, eliminates passport fraud, and reduces organizational overhead for stakeholders involved in verifying human knowledge documents.

The authors of the article "Blockchain, IoT and Fog Computing for Smart Education Management" [16] presented a great summary of the literature review of these techniques and, based on this review, applied modern technologies as an infrastructure for the development of educational innovations. Blockchain is used for recording and storing various collaborative data based on consensus in educational institutions, for developing teaching and learning on a digital platform, for storing information about student history, educational history in different grades, registration information, curriculum participation and institutional activities, academic performance and a certificate of education [16]. The Internet of Things and Fog Computing are used to develop infrastructure with the ability to create intelligent educational environments to support and quickly answer questions about the use of all types of equipment for real-time control. They allow to organize and share resources for collaboration work and training to gain access to the organization without restrictions on time or place.

Thus, the usage of blockchain technology in education is widely discussing for the last 5 years in the whole world, and in Ukraine particularly [17]. There is no doubt about the need to develop a strategy for the digital transformation of university education [18] with the modernization of the management of the corporate ecosystem, which should be implemented as a cloud platform. In this article, it is planned to streamline the considered methods and approaches to address the issue of creating an approach for saving intellectual and personal data involved in the training process in a reliable storage protected from the possibility of forgery and unauthorized access.

3. An approach for intellectual property assurance in digital university ecosystem

The process of transforming the educational environment in the format of "Smart Environment" [19] and striving for the realization of the idea of "Smart Pedagogy" is a new trend in the global educational field. Smart Pedagogy is a learning process in technology, different forms of information and media-enriched environment. This led to the fact that there is a lot of digital information which should be stored while the learning process in HEI and for a long time after its completion (Figure 1).

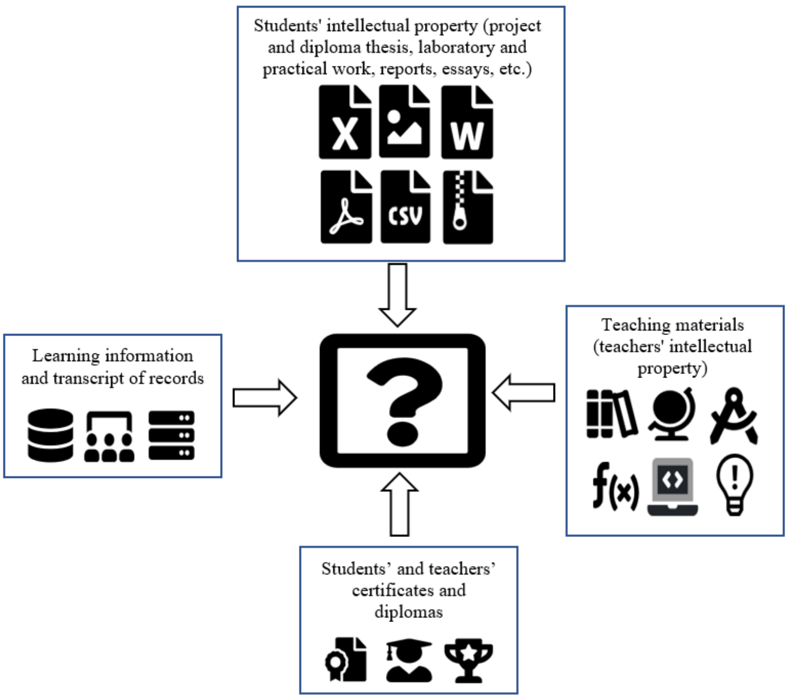

Figure 1: Data for integration in the university digital infrastructure

In the university digital ecosystem, it is very important to have a proper process of collecting, processing and storing the data about students' educational results which could confirm the level of the achieved outcomes within their study. The authors of the analyzed publications [12 - 17] agree about the need of using the blockchain to provide a reliable information network.

The blockchain is a database made up of a series of fixed-length blocks ordered over time, which could be integrated with applied information and communication technology in learning and teaching processes [20]. Each block contains one or more confirmed transactions. After a block has been verified and completed, it is added to the blockchain and all blocks are made public. The process of adding a transaction consists of:

1. Adding a transaction to a block. On average, blocks contain approximately 1 MB of information and are time stamped;
2. Cryptographic verification of each transaction;
3. Adding a new block after completion at the end of the block row, no transaction in the block can be deleted or changed (unchangeable) (as shown at the Figure 2, adding a new block fixes the hash of information from the previous block, which excludes the possibility of changing information in the previous block in the future).

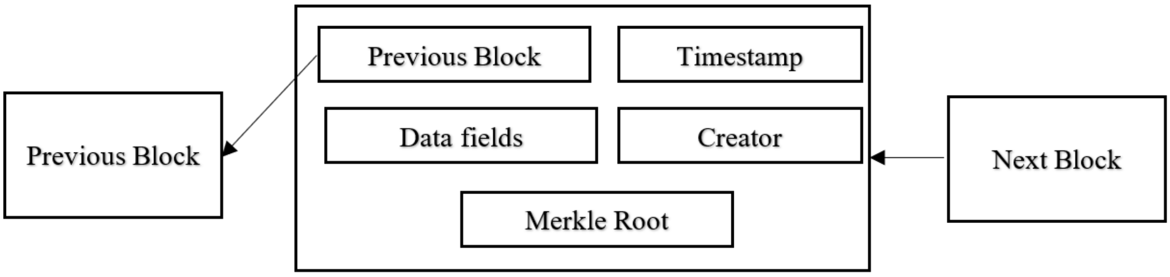

Figure 2: Blockchain structure

A Merkle root is a part of the block header and a simple mathematical way to verify the data on a Merkle tree. Merkle trees are an essential part of blockchain technology. A Merkle tree is a structure that allows for efficient and secure verification of content in a large body of data. This structure helps verify the sequence and content of the data. A Merkle tree summarizes all the transactions in a block by producing a digital fingerprint of the entire set of transactions, thus enabling a user to verify whether or not a transaction is included in a block [21].

The Merkle tree will be created based on the decision about what data and in what form should be stored in the blockchain.

Further consider the model for implementation of blockchain technology for intellectual property assurance in the digital university ecosystem.

3.1. Intellectual property assurance method for digital university ecosystem based on blockchain technology

Intellectual property assurance method for digital university ecosystem based on blockchain technology consists of the following steps:

- Step 1: Elicitation of the classes of the storing information. In this phase, all type of data which should be stored in the blockchain should be identified and separated into public and confidential.
- Step 2: Deployment of files storing and implementation of data transferring process into a file server.
- Step 3: Selection of the method and keys for encrypting private information and files.
- Step 4: Creating an interface system for uploading files and information into the blockchain with the LMS integration.
- Step 5: Storing information into the blockchain.

The first step is aimed to determine the information that needs to be stored to confirm the acquired skills and educational level, as well as for the management of the student's learning process itself.

Upon admission, the applicant must provide a document on previously received education and its supplementary, all required certificates, identity documents, a personal photo and other necessary documents. These documents must be stored in an encrypted way during the entire educational process, since contain confidential information.

After students are enrolled, the admission information is created – study degree, specialty/ educational program, form of study, type of financing, list of courses, etc. This information is public and must be available without encryption to confirm the enrollment process. The document that confirms this process is the enrollment order, a link to which can be attached to the enrollment record (the document must be publicly available).

The training process generates the following set of files and data:

- methodological support (should be publicly available with a link to authorship);
- learning outcomes in the form of completed project and diploma thesis (should be publicly available with a link to the owner), laboratory and practical work, reports, essays, etc. (must be in private access with a link to authorship);
- transcript of records – marks for all types of control and types of assignments (must be in private access with a link to the student and teacher);
- received learning outcomes (competencies and skills) (must be publicly available with a link to the student);
- student's and teacher's certificates and diplomas (should be publicly available with a link to the owner).

In the second step, it is proposed to store the files on a backup server, where each file will be assigned a unique number. Thus, a link to the file uploaded to the server will be saved in the blockchain. Depending on the file type, it will be stored in its original or encrypted form.

To encrypt private files, in the third step a unique key should be chosen, ideally which will uniquely identify the person who has access to this information. In each particular HEI, this key can be selected based on their own preferences. As an example, in Ukrainian HEI it is proposed to use identifiers from USEDE, i.e., person code in USEDE was chosen as the key for encrypting personal data and documents and education code in USEDE was chosen as the key for encrypting learning data and documents.

This choice depends on following factors:

- until the student is enrolled, there is no education code, but there is already a need to preserve the applicant's documents;
- a person can study in several programs (at the same time or not) and thus the use of an education code will allow separating this information, but at the same time personal information will not be duplicated (it is tied to the person code in USEDE);
- access to the person code and the training code has a limited circle of persons in the learning process (university administration);
- the graduate gets access to the education code (it is registered to the diploma supplement) for further demonstration of the training outcomes to employers.

In step 4 should be realized the integration with the used training platform to avoid data duplication and integrate the process of saving files and data into the blockchain without the need for additional actions from the participants of the educational process.

In the fifth step information which was elicitation at the first step should be saved into blockchain.

3.2. Implementation of the blockchain for intellectual property assurance method

A framework of the blockchain consist of the next layers, key ones of which will be described below:

- Data layer;

- Network layer;
- Consensus layer;
- Incentive layer;
- Contract layer;
- Application layer.

3.2.1. Data layer

At the data layer storing information about data block, chain structure, timestamp, hash function, Merkle tree and the encryption. The information shown in Figure 3 is entered into the blockchain transaction. The proposed blockchain architecture consists of the transaction head and the transaction data. The transaction data contains the nine columns where the data field carries information about the education process, such as the Creator, Leaner (person code), Education id (can be null), BLOB data (Smart Pedagogy Data), Transaction Type, File unique ID (from the file server), File hash (from the file server via SHA-256 cryptographic hash function), Outcomes, Mark. And the transaction head contains the four columns, such as the previous transaction key, the current transaction key, Merkle root (hash) and Date of creation (timestamp).

Transaction Type can be one of:

- Personal document (id = 1);
- Education document (id = 2);
- Intellectual property (learning outcome) (id = 3);
- Mark for learning activity (competencies and skills) (id = 4).

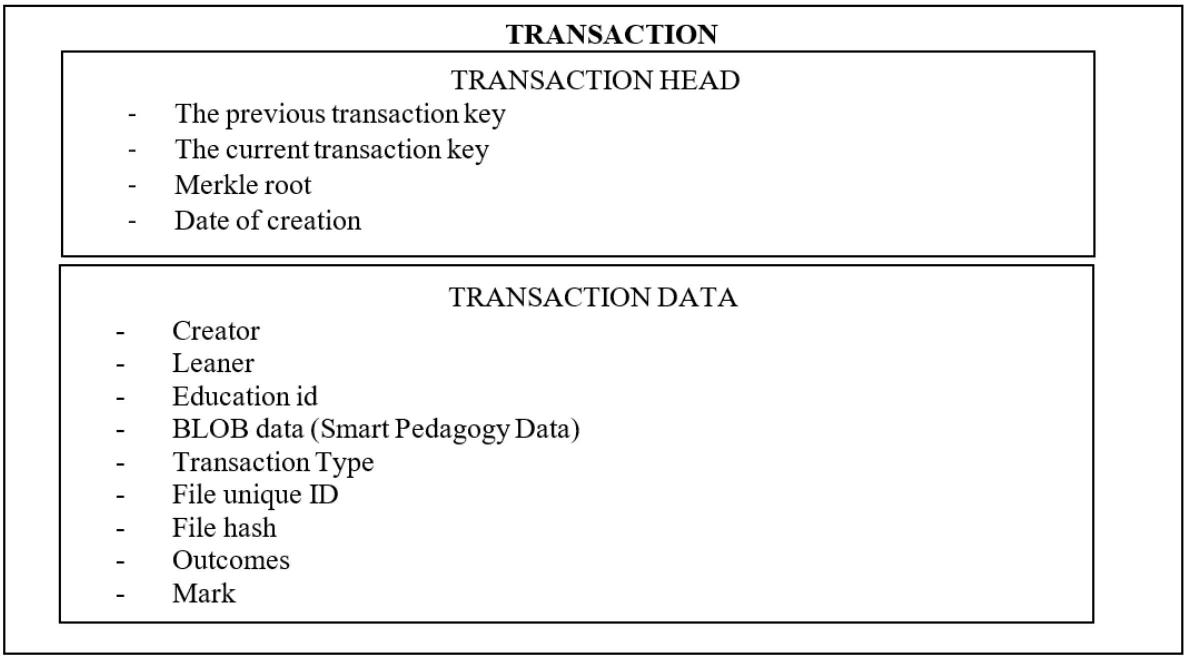

Figure 3: Transaction structure

For producing a digital fingerprint of the transaction propose to use the hash of the next data (Figure 4) using SHA-256 cryptographic hash function [22].

In the situation when the learner completed any activity for the second time, some documents should be updated on the server or any information should be changed, and results which were published in the blockchain before, this updated data will be uploaded and added into the blockchain again. Then all other nodes would have both the previous and actual assessment values for the same learner but with different timestamps (so the task of choosing the actual information will be the easiest).

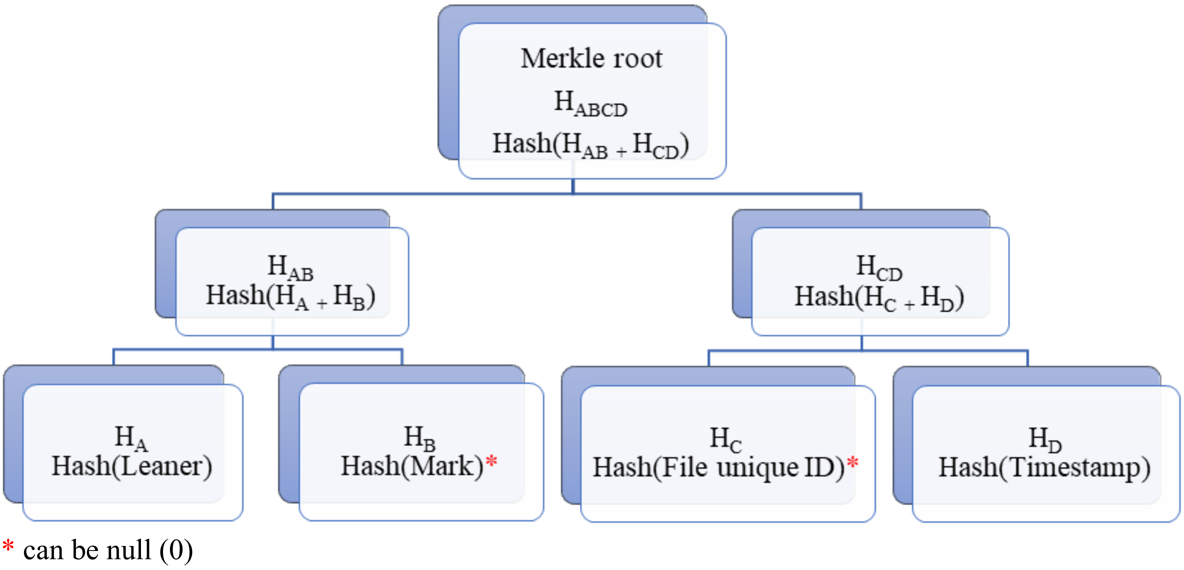

Figure 4: Merkle tree for learning information transaction

3.2.2. Consensus layer

The security of blockchain technology is achieved by the usage of the consensus algorithm. There are different types of consensus algorithms that might be executed before inserting a transaction in a block, comparison of which is presented in Table 1.

Based on the analysis of the advantage and disadvantages described in the Table I, the Delegated Proof-of-Stake (DPoS) consensus algorithm was chosen. According to this algorithm, selected delegates make the validation of the blocks by themselves. A relatively small number of delegates (about a couple dozen) can organize themselves efficiently and create designed time slots to publish blocks. With a collaborative effort and a partially centralized process, DPoS has been able to run orders of magnitude which are faster than any other consensus algorithms [23]. Also disadvantage of a partially centralized process in case of HEI's blockchain organization become the advantage on practice. Designing trusted delegates owned by the HEI as elected delegates will prevent a 51% attack when an attacker or a group of attackers gain control of 51% or more of the computing power or hash rate [24].

Table 1

Consensus algorithms comparison

Consensus algorithms name	Basis	Disadvantages	Advantages
Proof-of-Work (PoW)	Complex mathematical calculations	High CPU computations, is energy-intensive and costly	Highly scalable
Proof-of-Stake (PoS)	The PoS randomly selects validators, the higher chances of getting have the most coin holders	Complex implementations, vulnerable, only the richest can have control of the consensus	Higher speed, lesser energy consumption and hardware requirements
Delegated Proof-of-Stake (DPoS)	Selected delegates make the validation	A partially centralized process	Offers all the benefits of the PoS, faster than any other consensus algorithms, secure real-time voting
Byzantine Fault Tolerance (BFT)	Nodes regularly vote in order to identify the true transaction	There is no central authority that can step in to correct it, low scalability, semi-centralized system	High throughput, cost-efficiency, smart-contract support
Practical Byzantine Fault Tolerance (PBFT), SIEVE	This computation process asks the individual general about the opinion on the message	Susceptible to Sybil attacks, does not scale well	Forces a low overhead on the performance of the replicated service, energy efficiency, transaction finality, low reward variance
Proof-of-Weight (PoW)	Mechanism gives users a 'weight' based on how much cryptocurrency they are holding	Incentivization can be hard	Energy efficient, highly customizable and scalable
Proof-of-Burn (PoB)	By committing coins to an address where they are irretrievable, user earns a lifetime privilege to mine on the system based on a random selection process	The protocol wastes resources needlessly, mining power goes to those who are willing to burn more money	An interesting alternative to Proof-of-Work
Proof of Authority (PoA)	An optimized Proof-of-Stake model that leverages identity as a form of stake rather than actually staking tokens	Strongly lack decentralization, the risk of damaging the reputation does not necessarily keeps a person from participating in malicious actions	Low requirements for computational power, no requirement for communication between nodes in order to reach consensus, and the continuity of the network

3.2.3. Application layer

At the application level, the principle of interaction between applications and the blockchain is described. The process of saving student project thesis with IP data in the blockchain is shown in Figure 5.

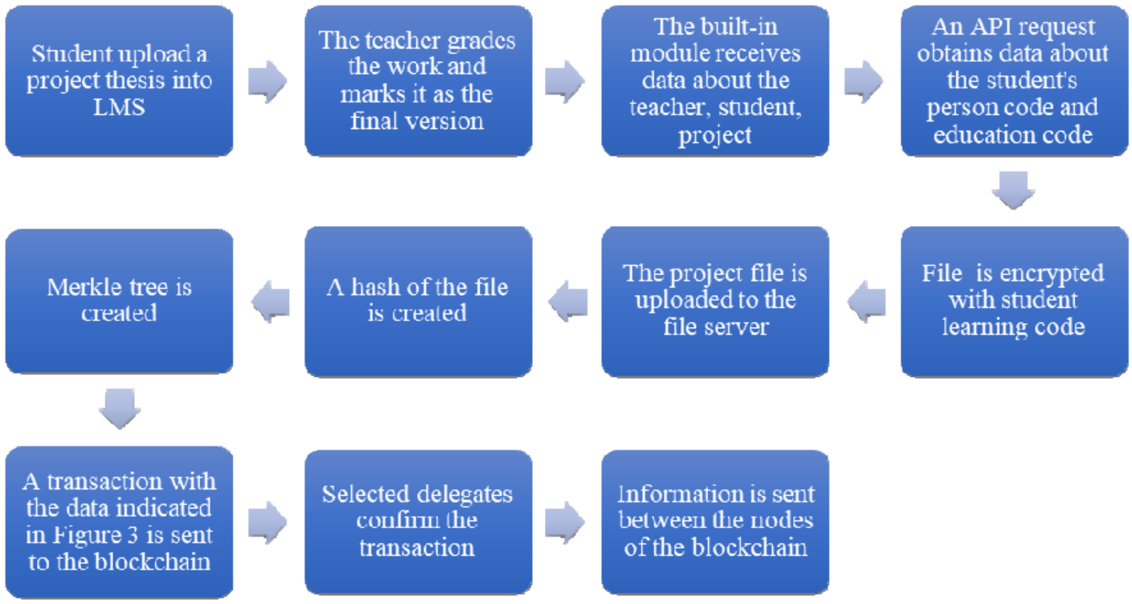

Figure 5: An example of loading a project thesis into the blockchain of intellectual property of HEI's participants

For application layer realization an interface system for uploading files and information into the blockchain should be developed. One of the features of this system is the LMS integration and API integration with the database with information about students and teachers. The LMS integration should be used for a simple, protected and user-friendly process of data and files transfer. API integration with the database is requested to obtain data about the student's person code and education code. The specification for the development of this system will depend on the LMS used in HEI and the access to the database with students' and teachers' information.

Taking into account the systems used in National University “Zaporizhzhia Polytechnic”, the following application integration is planned (Figure 6). It should integrate information from the university Moodle system, USEDE and data from the ECS eLearning Community Server, which is supporting international projects ViMaCs: Virtual Master Cooperation Data Science(ID: 57513461) [25] and Cross-domain competences for healthy and safe work in the 21st century WOR4CE [26].

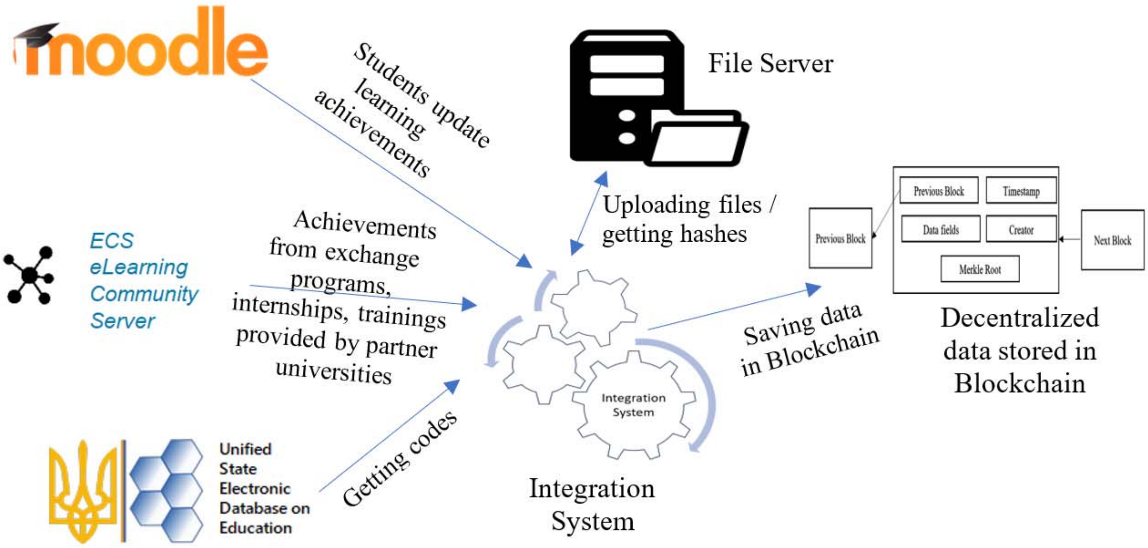

Figure 6: An example of the Application layer

4. Discussion

The proposed method can be used as a base for integration the data about students' educational achieved outcomes within their study and IP. In line with the hypothesis that digital university ecosystems are going to grow and expand the area of penetration, the application of this method can be used for different purposes, affording transparency and secure data archiving into infrastructure. The further implementation required integration of data from different sources so the cloud infrastructure of the ecosystem is also of great importance.

5. Acknowledgements

This research was partly done within the framework of international project "Cross-domain competences for healthy and safe work in the 21st century" (Ref. no. 619034-EPP-1-2020-1-UA-EPPKA2-CBHE-JP).

6. Conclusions

Intellectual property assurance method for digital university ecosystem based on blockchain technology was proposed in the article. The implementation of the proposed approach in different HEIs could become the basis for creation of the global cloud platform for intellectual property. It aimed to support the principles of academic integrity, afford transparency and secure archiving for intellectual property into university digital infrastructure. Based on the data stored in the blockchain it will be easy to confirm the presence of a diploma, learning competencies and skills, gained in the educational process, particularly the results achieved within alternative disciplines, training, internship as well as additional individual educational achievements.

7. References

[1] Order of the Ministry of Justice of Ukraine dated 12.04.2012 No. 587/5, 2012. URL: https://zakon.rada.gov.ua/laws/show/z0571-12#Text.
[2] About USEDE, 2020. URL: https://info.edbo.gov.ua/about.
[3] Welcome to UIS.Stat, 2021. URL: http://data.uis.unesco.org.

[4] Indicators databases, 2021. URL: https://www.oecd.org/education/database.htm.
[5] Education Statistics (EdStats), 2021. URL: https://datatopics.worldbank.org/education/indicators.
[6] Global Education, 2021. URL: https://ourworldindata.org/global-education.
[7] National Student Clearinghouse Verification Services, 2021. URL: https://nscverifications.org.
[8] Nuffic. The Dutch organisation for internationalisation in education, 2021. URL: https://www.nuffic.nl/en.
[9] How to verify the authenticity of a diploma, 2021. URL: http://www.insa-toulouse.fr/en/industrial/how-to-verify-the-authenticity-of-a-diploma.html.
[10] Prooftag, 2021. URL: http://www.prooftag.net.
[11] Documentorum, 2021. URL: https://exelor.net/documentorum.
[12] A. Mikroyannidis, A. Third, J. Domingue, A Case Study on the Decentralisation of Lifelong Learning Using Blockchain Technology, Journal of Interactive Media in Education 1 (2020) 23–32. doi: 10.5334/jime.591.
[13] P. L. Ogrutan, An Analysis on the Opportunity of Introducing Blockchain Technology in Education - A Case Study, TEM Journal (2020) 971-976. doi:10.18421/TEM93-19.
[14] H. Sun, X. Wang, X. Wang, Application of Blockchain Technology in Online Education, International Journal of Emerging Technologies in Learning (iJET) 13 (2018) 252-259. doi:10.3991/ijet.v13i10.9455.
[15] A. Arins, Blockchain arhitecture in Smart pedagogy, in: Innovations, Technologies and Research in Education, 2019, pp. 207-217. doi: 10.22364/atee.2019.itre.13.
[16] S. Chaiyarak, A. Koednet, P. Nilsook, Blockchain, IoT and Fog Computing for Smart Education Management, International journal of education and information technologies 14 (2020) 52-61. doi: 10.46300/9109.2020.14.7.
[17] O. Kaminskyi, Y. Yereshko, S. Kyrychenko, Digital transformation of university education in ukraine: trajectories of development in the conditions of new technological and economic order, Information Technologies and Learning Tools 64 (2018) 128-137. doi: 10.33407/itlt.v64i2.2083.
[18] G. Tabunshchyk, C. Wolff, P. Arras, Development of Cross-Domain Competences for Work 4.0, Springer Nature Switzerland AG 2021, M. E. Auer and T. Rüütmann (Eds.): ICL 2020, AISC 1328, 2021, pp. 205–211. doi:10.1007/978-3-030-68198-2_18.
[19] O. Kapliienko, S. Tabunshchyk, G. Tabunshchyk, T. Kapliienko, S. Sylenko, Virtual Reality Implementation for Design of Warehouse Lighting, in: The 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 18-21 September, 2019, Metz, France, pp. 969-973. doi: 10.1109/IDAACS.2019.8924272.
[20] O. Petrova, G. Tabunshchyk, T. Kapliienko, O. Kapliienko, Fuzzy Verification Method for Indoor-Navigation Systems, in: Proceedings of 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, February, 20 – 24, 2018, pp. 65 – 68. doi: 10.1109/TCSET.2018.8336157.
[21] Merkle Trees, 2017. URL: https://medium.com/hackernoon/merkle-trees-181cb4bc30b4
[22] H. Handschuh, SHA Family (Secure Hash Algorithm), in: van Tilborg H.C.A. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA, 2005. doi: 10.1007/0-387-23483-7_388
[23] What is Consensus Algorithm In Blockchain & Different Types Of Consensus Models, 2018. URL: https://medium.com/@BangBitTech/what-is-consensus-algorithm-in-blockchain-different-types-of-consensus-models-12cce443fc77.
[24] Understanding 51% Attacks On Blockchains, 2020. URL: https://www.jumpstartmag.com/understanding-51-attacks-on-blockchains/
[25] ViMaCs: Virtual Master Cooperation Data Science URL: https://go-study-europe.de/vimacs/
[26] WORK4CE: Cross-domain competences for healthy and safe work in the 21st century. URL: http://work4ce.eu/