Theoretical Aspects of Blockchain Technologies in The Sphere of Education

Antonina Liashkevych †, Mariana Babyshena †, Oleksandr Vorokhaev††, Volodymyr Pylypiv †††, Oksana Oliinyk††††, Nelia Kinakh†††††

maxnik8888@gmail.com

† Department of Social Sciences and Humanities and Innovative Pedagogy, Kherson State Maritime Academy

†† Postgraduate student of the Department of Social Work and educational and pedagogical sciences T.H. Shevchenko National University «Chernihiv Colehium»

†††Rector of the Kiev University of Culture

†††† Department of Hotel and Restaurant Business, Private Higher Education Institution "Kyiv University of Culture"

††††† Department of Pedagogy and Psychology, Volyn Institute of Postgraduate Pedagogical Education

Summary

The article provides a literary and analytical review in the following areas of search: problems and prerequisites for changes in the field of education, innovations and innovative models in education, the use of new technologies in teaching. A proposal for a business plan and accompanying documentation for a new methodology based on blockchain technologies were developed, to assess the economic efficiency of the project. The main systems of the new model were modeled on the basis of the proposed methodology, to develop a prototype based on the project documentation.

Key words:

Information technology, pedagogy, Higher Education, Education System, Technologies Blockchain, Methodology.

1. Introduction

In the context of economic and cultural globalization, the change of generations to "generation Z", a need is formed to integrate innovative technologies into the field of education, along with the principles of humanistic psychology. In modern Russian education, there is a lack of practical and project-based training, which, in addition to the rapidly aging material base of many educational institutions, leads to a discrepancy between the competencies and skills of students to generally accepted world standards and the real demand of the labor market.

The education system is a priority area of the internal policy of the state, since economic, social and technological development is closely related to the formation, preservation and increase of human capital, improving the quality of professional knowledge and skills of specialists. Timely response to global changes promotes faster adaptation to new conditions of scientific and technological modernization, the emergence of more effective social and technological innovations in schools and universities [3]. For example, the transition to the sixth technological order is aimed at the individualization of production and consumption, the development of new technologies for medicine, education and communications in order to increase the duration and quality of life of people. The technological structure, as a set of technical industries, presupposes not only a steady course of scientific and technological progress, but also the inertia of society's thinking [7].

Economic and cultural globalization is an important factor influencing the modern education system. Economic globalization leads to increased interactions between world economies, the involvement of countries in the international division of labor. Cultural globalization, in turn, is characterized by the formation of global information networks and the spread of various cultural models. The formation of an international educational environment (common educational space) was made possible by the signing of the Bologna Declaration on the European Higher Education Area in June 1999. ministers of education from 29 European countries. This declaration has become the main document that guides the signatory countries to form a common framework for the modernization and reform of higher education in Europe, including through the exchange of experience and extensive informatization, which leads to the emergence of a new type of economy - the "knowledge economy".

The purpose of the article is to develop a new methodology based on blockchain technologies to optimize, automate and increase the efficiency of the educational process for use at the university.

2. Theoretical Consideration

According to the results of the study [10], high unemployment among university graduates (more than 35%) is the result of the absence of a system for assigning students to jobs, there is a low competitiveness due to the need to adapt to real work, there is a discrepancy between the specialties in the university and the specialties that are really needed at the current labor

Manuscript received March 5, 2021
Manuscript revised March 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.3.25

market of the country. The education sector itself remains fragmented, where each educational institution provides services largely at the expense of its own resources, in some cases there is a low amount of funding from the state budget and insufficiently efficient allocation of budget funds [3]. The main task of education, as mentioned earlier, is the formation, accumulation and preservation of human capital.

The criticism of the existing reforms is in the following points [15, 16, 13]:

1. The ranking system used by the university may not provide the broadcast of educational innovations. This system can lead to the development of imitation activities, including the desire to increase the number of publications at any cost, often with a loss of their quality. Competition in this case can be reduced to the struggle for an administrative resource that oversees (often only imitates) the publication activity of employees.

2. Insufficiently effective implementation of the principles of the "Bologna system" (low accessibility and commercialization of education, a high shortage of specialists with a high need for highly qualified personnel in order to grow the world economy). This raises a whole range of questions about the training of teaching staff and the formation of a favorable environment for scientific and pedagogical activities, including an incentive policy of leadership in the field of regular advanced training of teachers in prestigious scientific organizations and leading universities in the world.

3. Problematic aspects of master's education:
   a) assessment of the results of mastering the main professional educational program;
   b) effective use of modern educational technologies;
   c) organization of an easily accessible practice-oriented educational environment.

Blockchain technologies fit into the components of innovative development in education: the development of the educational process, technical and technological development, and also have the characteristics of innovative educational models: the use of modern information communication technologies. Blockchain is an immutable public distributed data ledger that allows transactions to be carried out without a single central intermediary (decentralized network or peer-to-peer network consisting of nodes - individual users). If we consider in more detail - a built sequential chain of blocks containing encrypted or open information. Each block stores, in addition to information, its own hash-sum and the hash-sum of the previous block in the chain [8]. The most popular implementation of Blockchain technology is the Bitcoin cryptocurrency, proposed in 2008 and implemented in 2009. The system was created as a solution to the modern financial system, in which a small number of large banks control the issuance of invoices and the processing of transactions [1].

To quote the creator of Bitcoin Satoshi Nakamoto in this regard: “Banks must be trusted to hold our money and transfer it electronically, but they give it out in the form of waves of credit bubbles with a barely noticeable share in the reserve” (orig. “Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve ") [6].

To form the most complete picture, several additional definitions of this technology can be given [10]:

1. A decentralized ledger of all transactions in a peer-to-peer network, where participants can confirm transactions without the involvement of a certification authority (PriceWaterhouseCoopers, 2016).
2. Technology that provides secure and resilient management of distributed data, combined with data analysis techniques that add scalability and flexibility.
3. A distributed digital register of cryptographically signed transactions that are grouped into blocks.

Each block is cryptographically linked to the previous one after verification and consensus decision. As new blocks are added, older blocks become more difficult to modify. New blocks are replicated across all copies of the registry on the network, and any conflicts are automatically resolved using established rules. Thus, the blockchain technology is based on the concepts of a decentralized network architecture and uses a distributed data ledger governed by the established rules of the chosen consensus algorithm. Based on this, the blockchain has a number of the following properties [3]:

1. Decentralization. In a decentralized network, the need for a third controlling party disappears due to the equality of each of the participants and the functioning of the consensus algorithm, i.e. decentralization leads to complete consistency of operations (see further in the subsection “Consensus”).
2. Immutability. The blockchain is supposed to be an immutable data ledger due to its architecture. Each member's action (for example, a transaction) is

permanently entered into the register and cannot be changed.
3. Anonymity. Each participant is assigned an address that is used in the identity verification process. It is worth paying attention to the fact that the blockchain cannot guarantee the perfect preservation of confidentiality due to certain internal restrictions (see below in "Problems and ways to solve them").
4. Verifiability. The consensus algorithm (see further in the “Consensus” subsection) also allows an independent audit of the entire blockchain at a certain frequency and / or depending on certain conditions.

Traditionally, blockchain technologies are classified according to the degree of privacy: public, private (private) and hybrid (consortium) [5].

In the public blockchain, all records are available to the general public, and everyone can take part in the process of creating new blocks and auditing. As far as the private blockchain is concerned, only those nodes that come from one specific organization will be admitted to the consensus process. A private blockchain is viewed as a centralized network as it is completely controlled by one organization, only a small fraction of the nodes will be selected to determine the consensus. Hybrid blockchain (consortium) includes properties of the two types mentioned above. The comparison takes place in the following aspects:

1. Determining the degree of access to information and action.
2. Permission to read. Private blockchain transactions are invisible to the public.
3. Immutability. Since records are held by a large number of participants, it is almost impossible to falsify transactions on the public blockchain. In other words, transactions on a private blockchain can be easily tampered with since there are only a limited number of participants.
4. Efficiency. It takes a long time to propagate transactions and blocks as there are a large number of nodes in the public blockchain network. As a result, the number of blocks released per unit of time is limited and the latency is high.
5. Degree of centralization. The main difference between the three types of blockchains is that the public blockchain is decentralized, the hybrid blockchain is partially centralized, and the private blockchain is completely centralized. Additionally, you can give a classification according to the orientation of blockchain-based applications (dApps, see further in the subsection "Smart contract") for the financial and non-financial spheres. Financial blockchain applications include Bitcoin (cryptocurrency) and Ripple (cryptocurrency exchanger). The non-financial ones are Ethereum (a cryptocurrency with wide capabilities of smart contracts) and Hyperledger (a consortium of developers to create blockchain technologies for business) [5].

Blockchain has demonstrated its potential to transform the traditional industry with its key characteristics: decentralization, immutability, anonymity, and verifiability. The need to achieve consistency of actions (consensus) between blockchain users led to the creation of a solution in the form of various kinds of algorithms. The following is an overview of the typical consensus algorithms used in blockchain:

1. PoW (Proof-Of-Work, proof of work) is a strategy used in the Bitcoin network, the basis of which is a simple way - this is a random selection in a decentralized network of a user (he will be called a miner) who will be responsible for creating and auditing a new block. Since random selection is vulnerable to attacks, the selected user needs to do a lot of work (generating a block hash sum using the user's computing power) [4].
2. PoS (Proof-Of-Stake) is an energy efficient alternative to PoW. Miners in PoS must get the right to create and audit a block based on the funds on the balance sheet. It is believed that people with more currency will be less likely to attack the network. This method is more efficient than the previous one due to the lack of energy consumption. There is also an updated version - DpoS, in which a vote is taken to choose a miner from the list of proposed ones [6].
3. PBFT (Practical Byzantine Fault Tolerance) is an algorithm for solving errors of Byzantine generals [4], which can handle up to 1/3 of illegal attacks. A new block is determined in a round, in each round the primary one will be selected in accordance with some rules. The whole process could be divided into three phases: initial preparation, preparation and completion. In each phase, a node will enter the next phase if it received votes from more than 2/3 of all nodes, which contributes to a reliable choice of a leader who performs block creation and data audit.

Problems and solutions

Despite the great potential of blockchain technology, this technology faces numerous problems that limit the widespread use of blockchain [6, 23-25]:

1. Scalability. As the number of transactions increases,

the blockchain becomes cumbersome as each node has to store the entire transaction history. In addition, due to the initial block size limitation and the time interval used to generate a new block, Bitcoin can only process about 7 transactions per second, which cannot fulfill the requirement to process millions of transactions in real time. The following are some solutions to this problem:

a) Optimization of blockchain storage. Since it is more difficult for a single node to manage a full copy of a distributed ledger, a new scheme has been proposed in which old transaction records are deleted (or forgotten) by the network. The username database is used to store the balance of all non-empty addresses. A new scheme called VerSum allows high-weight clients to outsource expensive computations with large inputs. It ensures the correctness of the calculation result by comparing the results from several servers;

b) Redesign (refactoring of structure and architecture). The Bitcoin-NG cryptocurrency proposes to divide the usual block into two parts: a key block for electing a leader and a microblock for storing transactions. Once the key block is generated, the node becomes the leader, which is responsible for generating microblocks. Thus, the trade-off between block size and network security will hypothetically be eliminated.

2. Leak of confidential data. The blockchain can maintain a certain amount of confidentiality using public and private keys. However, the blockchain cannot guarantee the confidentiality of transactions, since the values of all transactions and balances for each public key are publicly available. To increase the anonymity of the blockchain, several blockchain projects have proposed the following methods, which can be roughly divided into two types:

a) Mixing. In the blockchain, user addresses are pseudo-anonymous. However, it is still possible to link addresses to the user's reality, since many users often transact with the same address.

A mixing service is a kind of service that provides anonymity by transferring funds from multiple input addresses to multiple output addresses.

Mixcoin offers an easy way to avoid dishonest behavior. The intermediary encrypts user requests, including the amount of funds and the date of the transfer, with his private key. Then, if the intermediary did not transfer the money, anyone could be convinced that the intermediary had cheated;

b) Anonymity. Zerocoin uses zero-knowledge proof. In order to prevent analysis of the content of transactions, miners should not verify the transaction using a digital signature, the source of payment should not be associated with transactions.

Humanity lives in an era of large amounts of data, the processing of which has become possible due to the high performance of modern computers and the development of effective methods for their processing (data science, machine learning, neural networks). Big data holds great potential as it can answer many questions in the context of business, economics, medicine and other fields.

In this regard, business stands out most of all, where companies such as Google, Amazon, Facebook use large volumes of information passing through them in order to better analyze users. Big data has many definitions. Specialists in the field of information technology define big data as large amounts of data that require large capacities for collection, storage, processing and analysis [6]. In addition, big data, in most cases, before processing contains a lot of unnecessary and damaged information [2]. The use of big data currently carries a lot of advantages, but it does not exclude certain problems when working with them, we list the main problems here [16-21]:

1. Volume. The volume of data generated by the population of the Earth is growing every day, in this regard, it is necessary to increase the capacity for their processing and analysis.

2. Variety. Data is generated over several channels in different forms, which leads to the need to create more advanced tools.

3. Speed. Currently, data from multiple sources can be accumulated at a rate comparable to the generation rate.

4. Credibility. Collected data may include outliers and false data due to the automation of their collection. With multiple sources, the situation gets worse. Big data is closely related to machine learning as a tool for processing and analyzing data in software.

Libraries such as Map Reduce and Apache Hadoop (HDFS) are used in this area as tools for distributed computing of large amounts of data in real time. Clustering, dimensionality reduction, forecasting are commonly used algorithms.

Examples of practical applications of machine learning include:

1) measuring the correlation between social attributes and the specifics of the crimes committed;

2) the use of uncontrolled (without human participation in checking the results of the analysis) methods for clustering groups of consumers of a certain product in a

retail network;
3) the use of controlled methods for forecasting weather in the regions of the country according to pre-compiled criteria. Most of the problems associated with the use of machine learning for processing and analyzing big data boil down to memory management (as noted earlier in the description of the main problems of using big data) [13-16].

It is of undoubted interest to consider big data in the context of the education sector. Big data accumulates naturally in the course of the activities of educational institutions: student data, scientific publications, etc.

The processing and analysis of big data in education provides quick results in assessing students' performance, makes it possible to accurately predict the future needs of students and makes it possible to make the necessary adjustments in the educational process in a modern way, and makes it possible to more effectively conduct comparative studies of the labor market and education in general.

The advantages are obvious and come from the results: improved academic performance, accurate distribution in educational programs, effective management [11-17].

Conclusions

In the course of the literary and analytical review, the prerequisites for global changes in the field of education, ways and innovative ways of optimizing and increasing the efficiency of the educational process, as well as increasing the level of employment of university graduates were identified. A complex of scientific articles and studies on the topic of gamification, blockchain technologies and big data was analyzed for further application in the field of education. The collected information confirms the feasibility of integrating the above technologies into the learning process of students, since it ensures the safety and immutability of data, automation of processes, and increased interest and motivation of students.

References

1 A.A. Verbitsky (2012). Active Learning in Higher Education: A Contextual Approach.
2 Zair-Bek E.S. (2010). Fundamentals of pedagogical design: a textbook for students, practicing teachers, St. Petersburg, p. 234.
3 Sergeev I.S. (2004). How to organize the project activities of students: A practical guide for employees of educational institutions, M., ARKTI, p. 4.
4 Smolkin A.M. (1991). Active teaching methods. M.
5 Kuts, M. O. (2016). Problem technologies in foreign languages teaching of higher technical educational establishments students'. Cherkasy University Bulletin: Pedagogical Sciences, 37(370).
6 Skliarenko Olesia, Akimova Alina & Svyrydenko Oksana (2019) Psycholinguistic Peculiarities of Contextual Realisation of Concept «MACHT» in Linguistic and Cultural Space of German's. Psycholinguistics. Pereiaslav-Khmelnytskyi Hryhorii Skovoroda State Pedagogikal University. 26 (2). pp. 321-340.
7 Shytyk Liudmyla & Akimova Alina (2020) Ways of Transferring the Internal Speech of Characters: Psycholinguistic Projection. Psycholinguistics. Pereiaslav-Khmelnytskyi Hryhorii Skovoroda State Pedagogikal University. 27 (2). pp. 361-384.
8 BogoyavlenskayaA. E. (2004). Development of students' cognitive independence, monograph, Tver, pp. 160
9 Rybnova A. N. (2002). System of management of professionally oriented independent cognitive activity of students, Saratov. state social – economy, Saratov, pp. 200.
11 Zimnyaya I.A. (1997). Pedagogical psychology, R., Phoenix, pp. 480.
12 Kovaleva T.M. (2009). Innovation school: axioms and hypotheses, Pedagogical community of Russia, pp.170.
13 Clarin M.V. (2010). Innovation in Learning: Metaphors and Models: An Analysis of Foreign Experience, pp. 300.
14 Lazarev, B.C., Martirosyan B.P. (2011). Pedagogical innovation: object, subject and basic concepts, Pedagogy, N 4.
15 Solodukhina O.A. (2011). Classification of innovative processes in education. Secondary vocational education, No. 10, pp. 12 - 13.
16 Yusufbekova N.R. (2011) General principles of pedagogical innovation: experience in developing the theory of innovative processes in education, M., pp. 90.
17 Novikova, T.G. (2009) Conditions for the effectiveness of innovative activity in education: foreign experience and a look at Russian practice, School technologies, No. 5, pp. 25-32.
18 M. Iasechko, M. Kolmykov, V. Larin, S.Bazilo, H. Lyashenko, P. Kravchenko, N. Polianova and I. Sharapa. (2020). Criteria for performing breakthroughs in the holes of radio electronic means under the influence of electromagnetic radiation, ARPN Journal of Engineering and Applied Sciences, 15(12), pp. 1380 - 1384.

19 M. Iasechko, N. Sachaniuk-Kavets'ka, V.Kostrytsia, V.Nikitchenko and S. Iasechko (2020). The results of simulation of the process of occurrence of damages to the semiconductor elements under the influence of multi-frequency signals of short duration, Journal of Critical Reviews, 7(12), pp. 109 - 112. doi:10.31838/jcr.07.13.18.
20 M. Iasechko, V. Larin, D. Maksiuta, S.Bazilo and I. Sharapa (2020). The method of determining the probability of affection of the semiconductor elements under the influence of the multifrequency space-time signals, Journal of Critical Reviews, 7(9), pp. 569 - 571. doi: 10.31838/jcr.07.09.113.
21 S. Piskunov, M.Iasechko, N. Minko , Yu. Dolomakin, O. Palagin, M. Musorina (2020). Taking Into Account The Correlated Errors Of Measurements When Estimating Parameters Of Object Trajectory At Mechanical Movement, IJETER, 8(9), , pp. 5603 — 5606. doi: 10.30534/ijeter/2020/112892020.
22 M. Iasechko, V. Larin, O. Ochkurenko, S. Salkutsan, L. Mikhailova, and O. Kozak (2019). Formalized Model Descriptions Of Modified Solid-State Plasma-Like Materials To Protect Radio-Electronic Means From The Effects Of Electromagnetic Radiation, IJATCSE. 8(3), pp. 393-398. doi: 10.30534/ijatcse/2019/09832019.
23 Romanenko, Y. O. (2016). Internet as a means of communication and its influence on public policy formation. Actual Problems of Economics, 175(1), 429-434.
24 Romanenko, Y. O. (2016). Place and role of communication in public policy. Actual Problems of Economics, 176(2), 25-26.
25 Hrusheva A. A. Strategies for managing educational institutions in terms of formation information society: coll. Science. Works. Inst. Of Pedagogy Academy of Pedagogical Sciences of Ukraine / AA Hrusheva - Formation of management competencies of university graduates: the experience of foreign countries, 2008.- P.68-77