

Application of Blockchain Technology in Higher Education

Nurilla Mahamatov
Department of Control and Computer
Engineering
Turin Politechnic University in
Tashkent
Tashkent, Uzbekistan
mahamatov@yahoo.com

Avaz Kuvnakov
Department of Information
Technologies
Tashkent University of Information
Technologies named after al-
Khwarizmi
Tashkent, Uzbekistan
avaz_a@yahoo.com

Bakhtiyor Yokubov
Department of Electronic and
Computer Engineering
Brunel University London
Uxbridge, UK
bakhtiyor.yokubov@brunel.ac.uk

Abstract— The development of fast-growing blockchain technology is encourages for the review and rethinking of many of the fundamental facts of our traditional education systems. As experience shows, the blockchain increases security and accessibility tremendously, such concepts as confidence, assessment and identity, currently doesn't satisfy users desires and there a reasonable necessity for the improvements. In this paper, we will consider providing of new methods for the database system in education, implementing the new blockchain technology in education since a new scheme can increase transparency and security in the education system.

Keywords— Blockchain, education, cryptocurrency, tokens.

I. INTRODUCTION

Recent advances in blockchain technology and decentralized consensus systems open up new possibilities for building untamperable domain-specific ledgers with no central authority. Since the launch of Bitcoin blockchains had been primarily used as a mechanism for value transfers [1]. With the growth of the Ethereum platform, the community realized that by using a chain of blocks and consensus rules one can not only store value and track its movement, but, more generally, store some state and enforce conditions upon which this state can be modified [2].

“Digital university admission application system with study documents using smart contracts on blockchain” proposes online a digital university admission application system with study documents and e-portfolio using smart contracts on blockchain in Ethereum platform. Additionally he noted that by using blockchain technology the system prevents the falsification of information and information leakage is prevented by combining with encryption [3].

Implementation of blockchain technology in education system” can be used to solve many educational problems and can help educators as well as learners to monitor the learning outcomes and the data can be stored securely and tamper proof format when it's stored onto then blockchain network [4].

Juricic, V. et al in [5] gives brief overview of current systems, their current state and a direction of their development, but also proposes specific guidelines and upgrades for current systems, that would enhance them and, consequently, the area of education. It also proposes blockchain integration levels in higher education that, combined with data extraction, can expand and deepen the area of education for the benefit of institutions, employers and students.

Bleir B. in [6] reports on the problems in primary and secondary school education that the Teachur project can solve. Its essence lies in a new approach for assessing students according to certain standards, a strict and secure system for storing this data, and in the ease of its transfer. The peculiarity of the innovative assessment system is that the assessment is associated with the knowledge and goals that were set at a given point in time, and the path of which is based on previous knowledge, goals and assessments, similar to how blocks in a blockchain are linked in chains, guaranteeing the safety and ease of transfer, while allowing you to evaluate more creatively and experimentally, in contrast, for example, from testing.

Bleir B. [7] describes four ways of applying blockchain technology in higher education implemented in the Teachur project: accounting for the learning process, smart contracts for obtaining a diploma, smart contracts for the bilateral market, Teachur platform tokens. The goals achieved during the training process are a reliable and complete report on the student's activities, which they can share at any time if they wish, which makes it easy to find employees and partners with the necessary skills. And getting a diploma is a smart contract that is executed automatically when the necessary conditions are met, which immediately becomes a reliable confirmation of the student's abilities. Teachers can receive deductions for a share or the whole part from the development and subsequent use of courses, educational materials, etc. The system implements its own tokens, which can be obtained just in the form of deductions or for another type of work. Thus, working with the system becomes economically viable.

Research on the use of smart contracts in the learning process was shared by Ben Blair in the article “Smart Contracts for Effective Curriculum” [5], where smart contracts are used for the entire curriculum when reaching a certain milestone in the curriculum - It is stipulated with a certain rigidly prescribed condition, and all educational materials are the intellectual property of their creator, for the use of which he receives deductions. Successful work on the educational materials of certain teachers increases the demand for them, which stimulates them to create high-quality materials.

Luke Parker wrote in the article “Authenticating about becoming the first to introduce blockchain to confirm the validity of candidate certificates and certificates for its compliance with the required competencies” academic certificates on the Bitcoin blockchain ”[6], which, in

essence, is a brief overview of the application of technology in this way.

Hereunder, we will try to briefly address the fundamentals and developments of this technology - including some of them in the specific education sector, and we'll try to insinuate a reflection and a debate which should address in the near future the impact, or not, of Blockchain in education.

II. METHODOLOGY

This section elaborates a number of consecutive steps required to be carried out throughout this research.

1. User Registration

In the learning process, there are times when the student begins to lag behind others in a particular discipline or even a number of disciplines, and if you do not react immediately, the lag will increase in subsequent stages, and problems will increase like a snowball.

It is not always possible to find the moment where exactly the problems started, because the information about the stages passed does not have easy access either from the teachers or the students. In the area of quick access, as a rule, there are only final results (assessments, certificates of successful completion, etc.), and often this will only be the latest data, and rolling back to an earlier stage becomes an almost impossible task.

In the described model, this task is proposed to be solved using the blockchain. Before starting work with the system, it is necessary to go through the registration process (Figure 1).

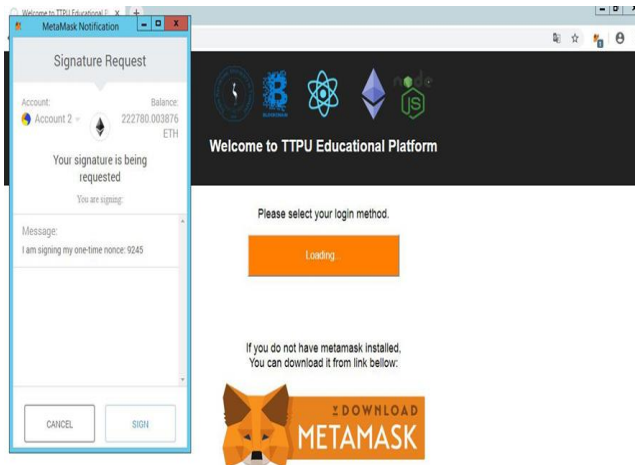


Fig. 1. Registration on Educational Platform.

At the first stage of registration, the user (whether it is a student or teacher) must generate a private key for himself based on any personal data or a combination of these. It is desirable that this is such information that will always be available, restored in the event of loss and unchanged over time. The students ID number was taken as an example, private key belongs only to the user. Based on it, using the encryption algorithm, a public key is created to which all personal information is attached (last name, first name, middle name, passport data, photo, user role in the system, etc.), and then it is confirmed in the educational organization. The introduction of personal data is the second stage of registration (Figure 2). Information about personal data is available only to the educational organization and the person who provided it.

Public keys are open and used by teachers to view and enter grades for a particular student in a block in the field with arrays of input data. The "block number" contains the block number in the chain in its strict sequence.

An element of the block "Achievement log" will act as an array of input data with data on the student's progress at certain stages when passing control points with fields of the following type: "Educational institution", "Student", "Discipline", "Control point", "Result", "Teacher", "Date".

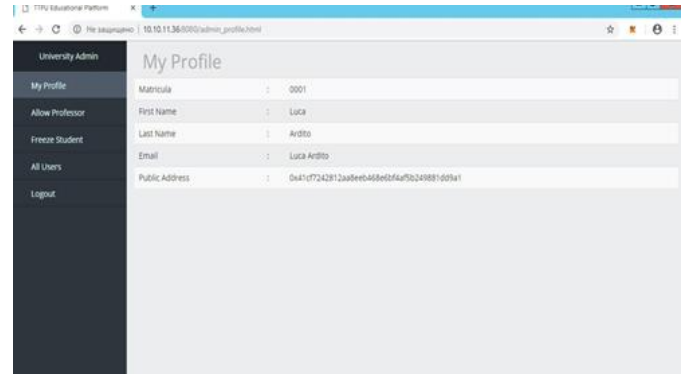


Fig 2. Personal Data

The Learner and Teacher fields will contain their public identifiers, not names or personal data (Figure 19). This will ensure the privacy of personal data from viewing from the outside.

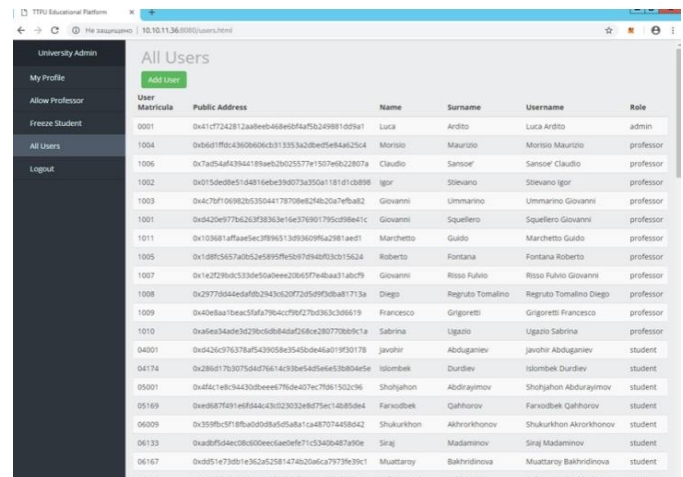


Fig.3. All Users Data

The fields "Discipline", "Result", "Date" contain information corresponding to their names without any encryption. Thus, each participant, knowing his public key, can find out the result of his activities at all stages passed.

The permissionless nature of our public chain leads to the ability for malevolent students to create educational institutes in order to get the scores for the courses they did not attend. Moreover, the knowledge students actually get by completing the course, and the conditions upon which the course is considered completed, vary significantly between the educational institutions. These issues currently cannot be solved solely on the protocol level: they require an external source of information to determine the physical existence and the reputation of an Educator. Although we leave the public chain open for the Educators to submit their private

block headers, we propose to add a separate layer of reputation and trust on top of the protocol.

We do so by disallowing a new Educator to join the network without an approval from another Educator. Educators are supposed to rate another Educators basing on off-chain sources of information – such as a publication on an official site of a university, which claims that given public key is issued by this university. By approving each other, Educators form a web of trust.

Ratings of Educators are backed up by ratings of Educators which trust them. The public elements of the block are “Block Number”, “Grade Journal”, “Previous Block” and “Hash”, which can be copied and checked for correctness (Figure 4).

Matricula	Public Key	Name	Surname	Email	Score
04001	0x5d26c5f79378a5439058a35450d46a019f00178	Jasorir	Abduganiev	Jasorir.Abduganiev	Mark
04174	0x2860176307504476614c33be54545e5304045e	Islombek	Durdiev	Islombek.Durdiev	Mark
05001	0x0f4c1e634430bee676de407c7081502c96	Shojjahon	Abdurayimov	Shojjahon.Abdurayimov	Mark
05169	0x6d887691e6544c43033032e8d75c14085d4	Fanodbek	Qahhorov	Fanodbek.Qahhorov	Mark
06009	0x359fb3cf8fb40d048a5d5a81ca48707445842	Shukurkhon	Akhrokhonov	Shukurkhon.Akhrokhonov	Mark
06133	0xadb54e0c8d00e0e5a0e7f71c340d487a90e	Siraj	Madaminov	Siraj.Madaminov	Mark
06167	0x051e73db1e362a52581474020a6ca7973939c1	Muattaroy	Bakhriddinova	Muattaroy.Bakhriddinova	Mark
06186	0x9870d63430118aef05daf153236563d974c	Safarmurod	Yulloshev	Safarmurod.Yulloshev	Mark
07020	0x17c17f4eaa7eaa1e3c522064aade3e0c27cc26	Islombek	jenbaev	Islombek.jenbaev	Mark
07021	0x9f2f2802dc82d9d9919105d282c5a0020a65	Abdubony	jonmirzayev	Abdubony.jonmirzayev	Mark
07022	0x9838ed0f1c98830ab4e451baf9353296597	Akbargon	jurayev	Akbargon.jurayev	Mark
07038	0xc4643af801085930a0664682d747e79a78d9	Behruz	Kuziev	Behruz.Kuziev	Mark
07041	0x6f4307f530783aa68f1a6dd11670334f0	Engash	Mashgarov	Engash.Mashgarov	Mark
07062	0x587933881e4c27975551c4e8f05005652464020	Abdulohitbek	Saydumarov	Abdulohitbek.Saydumarov	Mark

Fig.4. Course overview

Copies of block chains can be stored on many network nodes, ensuring the safety and consistency of students' data, and authorities controlling educational institutions to verify both performance indicators and the correctness of entering data will only need to have a copy of this chain.

2. Smart contracts

The system has the ability to technically access components such as:

- Parties to the contract - this is a student, teacher, educational institution;
- Subject of the agreement - between the student and the educational institution - this is a certificate or diploma of completion of education, between the teacher and the educational institution - this is the payment of wages.

And also analyze, measure and interact with such a component as a contract term. Between the student and the educational institution - these are indicators of performance, between the teacher and the educational institution - this is the effectiveness of teaching.

The decentralized nature of the blockchain allows you to do without a third party and to fulfill the agreement regarding the subject of the contract, as soon as all necessary conditions are met. Thanks to the digital signatures used on the blockchain, each action performed by the parties to the agreement will be confirmed and will then be verified.

Thus, the conditions described in the above are fulfilled for the work of implementing smart contracts.

We will directly register the provider of educational services and the contracting party, an educational institution, to which you can bind all the details of the institution (ID number, registration reason code, etc.). contact information, address and educational programs implemented.

As previously it was said that in the element of the block "Achievement Log" all the control points that the student passes will be stored. So, the educational program will be the stages that the student needs to go through and will include all the necessary components: content, goals, objectives, stages, curriculum and evaluating tools. For the teacher, however, it is necessary to make it possible to take the load, while the educational institution must form it.

As a result, the smart contract will be executed for the student upon successful completion of the control points laid down in the educational programs and described by the developers in the code, as a result of which a diploma or certificate with an electronic digital signature will be issued on the successful completion of training for a particular educational program. And for the teacher, the smart contract will work when the load is fulfilled, for the fulfillment of which he will receive a salary.

Due to the fact that the system will be open and at the same time act as a guarantor of the fulfillment of the terms of the contract, third parties will be able to find out what educational programs are implemented in the educational institution and how effectively they are implemented. Employers can, through a contact form, contact those graduates whose performance will satisfy their needs. Educational institutions can share educational programs between themselves and their affiliates.

3. Tokens

In order for the system to work stably, it is important that it is financially stable.

A new way to attract investment allows you to attract not only funds, but also a larger number of stakeholders who can contribute to the development of the organization. The system can create its own cryptocurrency of the organization, they are also tokens (Figure 5).

Using them, due to the presence of connections in the system it is possible to perform the following operations:

- Payment for training by students;
- Payment of salaries to teachers from the educational institution;
- Payment of scholarships to students from the educational institution;
- Other types of payments within the organization;
- Purchase of tokens of an educational institution for the purpose of investing it.

Thus, the system will have its own assets, depending on the indicators of their own activities, making the system self-sufficient. Educational institutions are interested in conducting educational activities efficiently, since the demand directly expressed in the price of their tokens will depend on this.

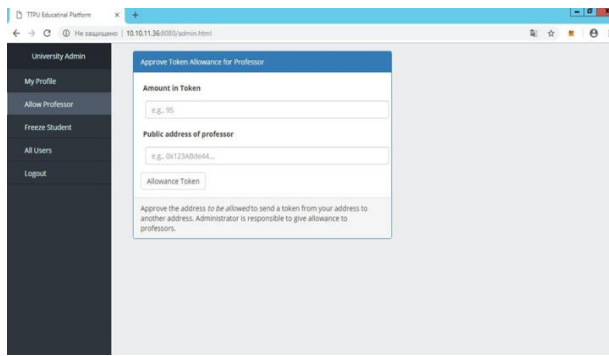


Fig. 5. System tokens

III. DISCUSSION

In order for the system to work stably, it is important that it is financially stable.

A new way to attract investment allows you to attract not only funds, but also a larger number of stakeholders who can contribute to the development of the organization.

The system can create its own cryptocurrency of the organization, they are also tokens. Using them, due to the presence of connections in the system, it is possible to perform the following operations:

- tuition fees The system is distributed, and its participants are equitable.
- However, it is still possible to highlight key roles, they are:
- Miners - participants whose role is to verify transaction hashes and then deposit them into the blockchain, for which they receive “Salary” in the form of a commission from transactions, as well as “mining” of a new cryptocurrency, which goes to those who, after checking the hashes of transactions and the next time a block is added to the blockchain, a new chain of blocks is created (the size of the issued cryptocurrency is limited);
- Developers - communities of those who are engaged in the completion, alteration, correction and “filling of holes” in the system, if any, to ensure correct and productive functioning, as well as security;
- Exchanges, exchangers, owners of popular wallets - these are organizations, persons and resources that allow you to purchase cryptocurrency in exchange for fiat money or another cryptocurrency;
- Ordinary users, customers of the system who want to purchase cryptocurrency, exchange it or transfer their funds to another user. As already mentioned above, the participants in the system are equal, so any user can play any of the roles.

On these main roles, as well as the features of the blockchain, you can try to build a system of education and science or some of the processes occurring in it. An approximate scheme of the blockchain-based system and its participants, transaction structure are presented in Figure 6.

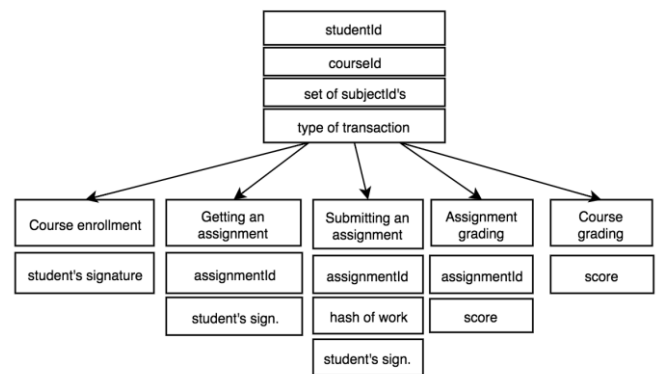


Fig.6. Transaction structure

To connect to the system, you need to create your own researcher identifier, which will be assigned to the studies when they are placed. Each block will also be assigned a unique digital signature (signature) so that data already entered cannot be changed, which ensures safety. The signature will be checked mathematically by all participants.

Since the unique digital signature is not tied to personal data, this will ensure anonymity. However, as in the case of cryptocurrencies, no one bothers to reveal their identity by indicating the identifier of the researcher as belonging to any person. Thus, they will also be able to work on certain studies, uniting into groups (groups of researchers, educational organizations, etc.). Moreover, in this case it will be possible to work in your own name or in the name of the organization.

The participants in the system will verify the research for authenticity by indicating those blocks or even entire chains of blocks that have already been verified earlier, where the information is refuted or confirmed. Then, the rest of the validating participants, on the basis of this check, confirm or reject the inclusion of the block in the blockchain.

For block verification, participants will receive rewards in the form of tokens that will allow access to the block for its verification, for the possibility of publishing the study and which will have a real price, which will ensure the financial stability of the system. It will be possible to exchange or purchase tokens on existing exchanges and exchangers (provided that the system gains popularity and exchanges with exchangers start working with them).

Authentication of blocks will be available only to certain participants to prevent mass confirmation of inaccurate studies by incompetent users. The selection criteria for examiners may include: the number of studies released, the volume of blocks tested, etc.

To limit the publication of blocks, a rating system can be applied in which a participant with a certain identifier, whose studies are not regularly confirmed, will have to pay more and more tokens each time in order to be able to submit his research for verification. This will reduce the load on the system.

So, it's worth summarizing to determine the advantages and disadvantages of the system. Researchers will be interested in publishing reliable studies so as not to pay a large commission for the possibility of introducing their research into the blockchain and receive great benefits for successfully completed research.

Token holders will have a valuable product, as well as the ability to “mine” (mine) by checking signatures and confirming or rejecting the verification. The first ones to correctly check the block will receive the greatest benefit, which will ensure the speed of operation and the relevance of the data. Participating developers will be interested in ensuring that the system functions correctly and is safe, and that their tokens are safe. Based on the foregoing, we can say that the system meets the requirements of self-regulation.

Each participant, if desired and perseverance, can play any of the roles, which means that we can talk about the equality of participants.

Since the blockchain will contain a huge base of only the most relevant research, it will attract more new participants to purchase tokens in order to gain access to such a “storehouse of knowledge”. Now, to search for the necessary information, it will not be necessary to sort through tons of information, but just connect to the system. All this will ensure accessibility, transparency and freedom in scientific improvement.

Perhaps the system looks a little utopian, because the participants may not be interested in checking the blocks, or the researchers will not want to pay for the opportunity to make their research, or the signature verification will not be financially attractive, however, the advantages and potential of the technology, and Also, the opportunity to benefit may be an incentive for development.

It should also be understood that not every research has the right to become public knowledge, since it can harm a person or the environment, so there must be some filter for compliance with the law and, possibly, some moral standards that already apply to ethical issues.

IV. CONCLUSION

The paper described theoretical models for the implementation of two scenarios for the application of blockchain technology: in education and science. The scenario of using blockchain technology in education is an approach to this area through the conduct of a performance journal, thanks to which it is supposed to track all the student's academic results at all stages of his education, thus creating a complete picture of his activities. This will reveal the strengths or weaknesses of the student, roll back to the moment when misunderstanding began, even if it was a very long time ago, and thereby adjust the learning model and fill the gap in the student's knowledge.

V. FUTURE WORK

The Currently, in the educational system like in other spheres, trends change year by year. Technology is developing faster than ever, which leads to a change in the importance of different professions in all areas of work. The educational system also cannot always provide relevant training programs, which sometimes become outdated even before graduates receive diplomas. With the creation of a system that would allow you to see the requirements for specialists in real time, an understanding would come of what changes in the education system should occur. Moreover, this would lead to a simplification of the search for vacancies and the fight against unemployment among educated people. Such a register based on blockchain is

necessary for universities, graduates, employers, and the education system.

The options for using the blockchain in the education system are not limited to storing documents in a database. All the advantages of this technology can radically change the education system, for example, contribute to online learning. If we could to combine the various courses in blocks, then we can develop training areas in many highly specialized specialties, standards should be developed for the blockchain which will allows for the recognition of any diplomas and certificates anywhere in the world.

REFERENCES

- [1] S. Nakamoto “Bitcoin: A peer-to-peer electronic cash system” 2008.
- [2] G.Wood. “Ethereum: A secure decentralised generalised transaction ledger” Ethereum Project Yellow Paper, 2014. 151 1-32.
- [3] K.Mori and H.Miwa. “Digital university admission application system with study documents using smart contracts on blockchain”, 2020.
- [4] A.S.Karale and H.Khanuja “Implementation of blockchain technology in education system”. International Journal of Recent Technology and Engineering, 8(2), 2019. pp. 3823-3828.
- [5] V Juricic, M Radošević and E. Fuzul “Creating student's profile using blockchain technology”. 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2019 - Proceedings, 2019. pp. 521-525.
- [6] B.Bleir “Using blockchain to re-imagine learning”, <https://medium.com/@KnowledgeWorks/using-blockchain-to-re-imagine-learning-fb3bf2717b>
- [7] B. Bleir “4 Use Cases for Blockchain for Higher Ed”, https://medium.com/@benblair_34530/4-use-cases-for-blockchain-for-higher-ed-afec2fc9b49
- [8] B. Bleir “Smart Contracts for Effective Curriculum”, https://medium.com/@benblair_34530/smart-contracts-for-effective-curriculum-30c610067c51
- [9] L. Parker “Authenticating academic certificates on the Bitcoin blockchain”. <https://bravenewcoin.com/news/authenticating-academic-certificates-on-the-bitcoin-blockchain/>

