The Main Aspects of Application of Blockchain Technology in the Educational Process [*]

Dmitry Mouromtsev [0000-0002-0644-9242], Ilia Gosudarev [0000-0003-4236-5991], and Stanislav Sivinskiy [0000-0003-4167-1081]

ITMO University, 49 Kronverksky Pr., 197101 St. Petersburg, Russia
d.muromtsev@gmail.com, goss@itmo.ru, stanislav_sivin@mail.ru

Abstract. The architecture of interaction organization between LMS and blockchain technology is proposed in the article. The issue of identification of students with the purpose of possibility of application of adaptive methods of training is considered. Existing methods of authentication of listeners realized in system Moodle are considered. The methods of increasing student identification through the introduction of biometric algorithms are proposed. The existing libraries of identification are considered and the module of recognition of the user by means of a web camera (a laptop or a smartphone) is realized.

Keywords: LMS, Moodle, identification, authentication, private key, public key, face recognition

1 Introduction

At the present stage, the development of information technology has led to the need to store a large number of valuable information. It is often necessary to restrict access to stored information only to a certain number of persons who have the necessary set of input data to pass the authentication procedure. The requirement to restrict access to information follows from the Federal law 152 "About a personal data» [1].

Of great importance is the need for authentication in learning management systems. The first prerequisite is the need to distinguish between the activities of the teacher and the student at the LMS, as well as the possibility of encapsulating the environment of students only the information space of the course and contacts with the tutor of the course.

In accordance with GOST P53632-2009, authentication is a process of confirming the claimed identity to ensure that the established identity of the user is correct [2].

The Moodle learning management system uses several authentication options, among which we can highlight: authorization through login and password; authorization based on a public-key.

2 Authorization through login and password

The simplest and most common authentication method is the login and password authentication method. This method is widely used for authorization on many websites.

Let's consider the implementation of this method in the distance learning environment. The Moodle database structure contains the table "mdl_user" (by default, the prefix mdl_ is added during deployment). This table is one of a group of tables describing users and their profiles [3].

The key fields for authorization in the Moodle system are the "username" and "password" fields.

It should be noted that in order to increase the security level of user passwords storage, the final presentation of the password is saved in the form of an encrypted string: "$2y$10$rloxabsylvwgEBIZoKXHju.YxRTQchKBUcIzKK1VCn6mfppYRdk.C".

Starting with Moodle 2.5, the policy of using salt to encrypt passwords has changed. If before version 2.5 salt was created once and applied to all passwords on the web-site, it led to reducing of the level of security and its effectiveness, then since version 2.5 Moodle relies on the possibility of bcrypt [4] programming language PHP 5.3.7 module and generates a salt randomly each time unique for a new password. If we try to install Moodle version 2.5 or higher in an environment where the PHP language version is lower than 5.3.7, the system will revert to the old password saving method [5].

Let's consider in more detail the structure of the stored string:

- $2y$ - identifier of the hash algorithm was used. In this case, the algorithm (CRYPT_BLOWFISH) compatible with the crypt () function.
- 10$ - the required algorithmic complexity.
- RlOXAbSYLVWGE-22 characters of salt
- BIZoKXHju.YxRTQchKBUcIzKK1VCn6mfppYRdk.C – the hash of password

The disadvantage of this approach is the huge accumulation of different logins and passwords for different web-sites and systems, as well as the need to fill out a user's account with a name, e-mail, phone, address, etc. Combining OpenID[6] and OAuth[7] allowed to solve this problem. An example is the registration of a user in Google and the further possibility of authorization through Google on the web-sites. Google in this case acts as a provider with OpenID service, and the implemented OAuth mechanism acts as a tool for organizing authorization. Today, some software developers for Moodle provide ready-made solutions for the organization of such authorization through social networks [8].

3 Web services and authorization through a token

The LMS is available as web service starting with Moodle version 3+. By default, only one service is available in the system "Moodle mobile web service". On the basis of the use of all the functions provided by this service, the Moodle mobile application functions [9].

Web services can be accessed via the following protocols: REST, SOAP, XML-RPC. The most popular protocol is the REST protocol. The advantages of this protocol are performance and scalability.

Before users start using the protocol, they must activate it in the Moodle LMS settings [10].

Next, they need to create a public key (token) by entering user data, selecting the service and setting the token expiration date, after which the key will be considered invalid.

The disadvantage of this approach is the constant need to notify users about the change of the key, and if the key is compromised, the system becomes vulnerable.

When organizing distance learning, a number of issues arise, among which we can highlight the issue of user identification, this issue becomes especially relevant when we are implementing adaptive learning. And in terms of the possibility of transferring the login and password or token to a third party, all efforts to adapt the level of complexity of the task and build an individual educational trajectory become meaningless.

4 The problem of identifying the user

The organization of distance learning raises a number of issues, including the identification of users and the problem of "cold start".

The problem of user identification becomes especially actual in the process of applying adaptive learning algorithms. Under the conditions of the existence of the possibility of transferring the login and password or token to a third party, all efforts to adapt the level of complexity of the task and to build an individual educational trajectory become senseless.

One of the most effective methods of user identification is biometric technology.

In comparison with access passwords, individual keys and cards, biometric identification has the following advantages: biometric characteristics are part of a person, so they cannot be forgotten or lost; biometric identifier cannot be passed on to another person; tampering with the "biometric key" is significantly hampered; contactless biometric technologies have an increased ease of use.

Tools for recording physiological parameters (pulse meters, eye-tracker movements and brain-neuro-interface activity) can provide fairly accurate results.

The most promising in this direction are the neuro-interfaces, which are systems created to organize a protocol for data exchange between the brain and the computer system. The fields of application of neuro-interfaces are very different from military and medical to educational purposes [11,12]. The use of neuro-interfaces is based on the process of registration of brain electrical activity (electroencephalogram (EEG)).

Examples of neuro-interfaces are: Muse (https://choosemuse.com/); EPOC+ (https://www.emotiv.com/epoc/); Neurochat (http://neurochat.pro/); MindWave (https://store.neurosky.com/); FocusEdu (https://www.brainco.tech/).

Measuring the physiological parameters of the learner in the future will not only help to identify the learner with sufficient accuracy [13], but will also help to solve the problems of customization for individual cognitive style and provide appropriate (relevant) cognitive load for each learner, allowing the transition from individualization to adaptive e-learning.

The disadvantages of neuro-interfaces include a rather high cost of equipment, which in the conditions of mass learning becomes inaccessible to most trainees, which in turn makes it difficult to apply such technologies in the educational process.

Also among the existing methods of user identification is the ability to recognize faces in real time using a web camera (laptop or smartphone) [14].

The authors of the article highlight two existing areas of facial recognition applications available to developers: Software as a Service (SaaS) and standalone libraries for programming languages.

Let's consider the existing SaaS solutions for face recognition.

Kairos (https://www.kairos.com/) - the platform offers a wide range of solutions for image recognition. API includes sex, age, emotional state, face recognition in photos and videos and much more.

EyeRecognize Face Detection (https://rapidapi.com/eyerecognize/api/face-detection-and-facial-features) - provides coordinates for all detected faces and associated features such as eyes, nose, mouth, skin color and hair color. Also under development is the ability to assess gender, race and age.

BetaFace Face Recognition (https://www.betafaceapi.com/) - provides the ability to detect, analyze, recognize and compare faces, create your own face databases or use public databases. It supports gender, age, facial expression, ethnicity, adult content, 22 + 101 mimic reference points and more than 40 facial attributes.

The second area of facial recognition is the use of libraries in the development process. In the field of development of facial recognition software in the JavaScript programming language, the authors of the article highlighted the following libraries:

tracking.js (https://trackingjs.com/) - provides various algorithms and methods of computer vision in a browser environment. Using modern HTML5 specifications, it is able to track colors in real time, recognize faces, while having an intuitive interface.

face-api.js (https://github.com/justadudewhohacks/face-api.js/) - JavaScript library implemented on the basis of tensorflow.js kernel providing facial recognition capabilities. Provides the ability to run both on the client side, and based on the Node.JS platform Face-Api.js supports the following basic features detect and recognize faces, expressions, age, gender.

face-recognition.js (https://github.com/justadudewhohacks/face-recognition.js) is a library for reliable face detection and recognition. The library is a wrapper over face detection and recognition tools implemented in the dlib library written in C++.

5 Blockchain. Basic stages of development

A blockchain is a continuous and sequential chain of blocks built according to certain rules. Relationship between blocks is provided not only by numbering, but also by the fact that each block contains a hash sum of its own block and the previous one. The hash function is formed by applying the Ethash algorithm (SHA-3) with submission of block number, the value of the hash function of the previous block and the information stored in the block. Thus, if you make changes in the information field of one of the blocks, all subsequent blocks in the chain automatically become non-valid.

Blockchain as a technology has passed several stages of development.

The first stage is the release of the article "Bitcoin: A Peer-to-Peer Electronic Cash System" on October 31, 2008 by Satoshi Nakamoto, who developed and released the protocol of Bitcoin cryptovoltaics.

In the second stage of BitCoin development, the technology found its application not only as a cryptovoltaic currency, but also as a means of reliable, decentralized and invariable storage of user data. The most prominent projects of the blockchain technology at this stage are Ethereum, Hyperledger Fabric, Corda. The main innovation is the ability to write smart-contracts (in the narrow sense of functions for data processing). For the first time smart-contracts became widespread with the advent of Ethereum in 2013 and further development of Vitaly Butlerov's idea about the possibility of using block technology as a universal decentralized platform for the implementation of information storage and processing system.

The authors see the next stage of the blockchain technology development as an opportunity to solve the scalability problem. The essence of which is to limit the volume of stored data in one block not more than one megabyte. In view of the peculiarities of the blockchain architecture, which requires a constant transfer of data, such a solution is logical in view of reducing the effectiveness of potential DDoS-attack. But due to the increase in the number of network members and the volume of stored data, the speed of processing requests and queues are forced to sink. Since 2017, active development of possible solutions has been underway. Among which it is possible to allocate: Segregated Witness (SegWit), Bitcoin Cash, SegWit2x.

6 Opportunities of blockchain in the educational process

The authors of the article see the possibility of the introduction of blockchain technology, Ethereum, for example, [15] to model the interaction of teacher, students and LMS (Moodle as an option).

The use of blockchain technology provides the possibility of reliable storage of Moodle events without the possibility of their modification. In case of altering the data in the Moodle database, the fact of alteration will be immediately visible, because the blockchain acts as a reference point for checking the correctness of the data stored in the database.

With the ability to log the history of user interaction with the LMS in the form of blocks and executing the chain of actions from the smart contract, it becomes impossible to fake user activity. And at a certain level, it becomes possible to increase the level of user authentication, by binding devices to LMS [16].

Let's consider an example of application of such interrelation on an example of system of remote training of the educational office of Computer Design and Design (design.ifmo.ru) at ITMO University: desginifmo.ru.

Base system of remote training is system Moodle of version 3.5. Using the built-in possibility of logging the events taking place in the system (user authorization, viewing the course, viewing the task, sending a response, trying to perform a test), the ReportAction plugin was developed with the support of the possibility of launching the task in the scheduler via cron.php, in order to call a smart contract to record new events taking place in the system.

An online wallet was used to include the user in the blockchain network in order to store the private and public keys of listeners.

According to figure 1, the communication scheme of the modules and the process of recording the response event are presented.

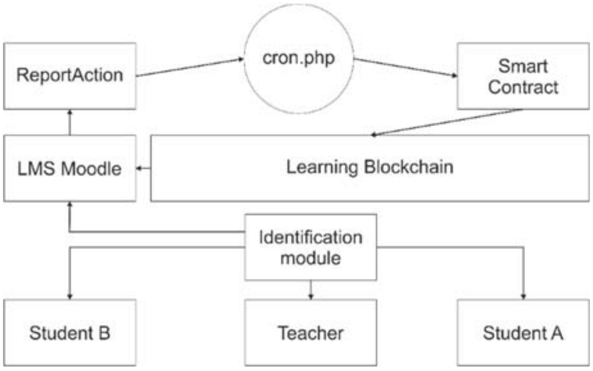

Fig. 1. Communication scheme of the main modules based on blockchain technology

In general, the recorded data in the blockchain is a JSON structure:

{time: 1579890444, user: "0xff2999f3335ea354906cd103eb5bdb3991e", relateduser: "0xf83d4e53a82e3cdbc95c74d843d76dd46e963766", action: "send answer", module_id: 68, level_credo: 0.57}

The identification module included in the scheme is another level of user identification verification through biometric data. The module supports only face recognition of listeners and recording of probability of matching in the level_credo variable. The module's operation is based on face-api.js. The module developed today operates in test mode and is of recommendatory character.

According to Table 1, experimental data obtained during testing of the developed module are presented.

Table 1. Results of student recognition

Student	Score (max = 1)	Middle score (max = 1)
Student A	0.47	0.49
	0.48	
	0.51	
Student B	0.43	0.44
	0.49	
	0.42	
Student C	0.55	0.53
	0.54	
	0.5	
Student D	0.43	0.42
	0.42	
	0.42	

Several factors affect the success of the module: the quality of photos that are submitted to the input of the neural network as reference, the number of photos and displaying various emotions.

Application of blockchain technology in combination with the module of identification of students on the basis of biometric data allows to speak about the improvement of the quality of interaction with students and provides an opportunity for a favorable introduction of methods of adaptive learning in the educational process. Due to the absence of strict formalization of data storage in the blockchain, this format of data storage opens the prospects of the evolutionary approach to the introduction of models of adaptive learning without correction and cardinal restructuring of the system of data storage of students.

Also, the use of blockchain technology opens up the possibility to consider courses with which users interact as independent participants in the process. In [17] it is stated that the introduction of blockchain technology will solve the problem of "cold start" in adaptive learning when the student moves from one educational organization to another, due to the possibility of obtaining the entire chain of information through the blockchain. In our opinion, the problem of comparing the correspondence of the educational information of the course with what is studied in the new educational organization remains. The main reason is an educational topic can be disclosed from different points of view.

The solution of the problem is the need to look at the educational course as a full participant in the learning process. Namely, the course must have opportunity to sign in digital form its activities with users of the system.

7 Conclusions

Application of the block technology will allow to organize reliable and invariable data storage and, due to the absence of a strictly limited data presentation scheme, creates prerequisites for the development and implementation of new methods of adaptive learning without changing existing developments.

Application of biometric identification methods allows increasing confidence in the identity of the user and creates conditions for the correct application of adaptive learning algorithms.

The innovation connected with the provision of the training course with the possibility to sign the actions independently will allow transferring the course from one system to another without losing the identification, since the number of the primary key in the database becomes redundant. Also, by creating backups and logging changes in the course, it will be possible to recreate the appearance of the course at various stages of interaction with it in order to compare the course content of different educational organizations.

References

1. Federal'nyj zakon "O personal'nyh dannyh" ot 27.07.2006 N 152-FZ (poslednyaya redakciya), http://www.consultant.ru/document/cons_doc_ LAW_61801/. Last accessed 28.12.2019
2. GOST R 53632-2009. Pokazateli kachestva uslug dostupa v Internet. Obshchie trebovaniya, http://docs.cntd.ru/ document/gost-r-53632-2009. Last accessed 28.12.2019
3. Moodle. Database schema introduction, https://docs.moodle.org/dev/ Database_schema_introduction. Last accessed 28.12.2019
4. PHP. Function password_hash, https://www.php.net/manual/ru/function. password-hash.php. Last accessed 28.12.2019
5. Moodle. Password salting, https://docs.moodle.org/37/en/Password_salting. Last accessed 28.12.2019
6. OpenID, https://openid.net/. Last accessed 28.12.2019
7. OAuth2, https://oauth.net/2/. Last accessed 28.12.2019
8. LenAuth Plugin, https://lmstech.ru/lenauth-plugin-oauth-moodle/. Last accessed 28.12.2019
9. Prilozheniya v GooglePlay. Moodle Mobile, https://play.google.com/store/apps/details? id=com.moodle.moodlemobile&hl=ru. Last accessed 28.12.2019
10. MOODLE REST WEB SERVICES TUTORIAL – EXAMPLE – INSTRUCTIONS – GUIDELINES, http://www.spanidis.eu/?p=27. Last accessed 28.12.2019
11. Kazhdomu shkol'niku po bol'shomu bratu, https://stimul.online/articles/sreda/kazhdomu-shkolniku-po-bolshomu-bratu/. Last accessed 28.12.2019
12. Brainco wants to improve China’s education with a brain-machine interface wearable, https://technode.com/2017/01/17/brainco-wants-to-improve-chinas-education-with-a-brain-machine-interface-wearable/. Last accessed 28.12.2019

13. Lyamin A.V., CHerepovskaya E.N. Eksperimental'nye issledovaniya biometricheskoj identifikacii pol'zovatelej na osnove dannyh ajtrekera tobiix2-30 // Informacionno-upravlyayushchie sistemy. 2015. №5 (78), https://cyberleninka.ru/article/n/eksperimentalnye-issledovaniya-biometricheskoy-identifikatsii-polzovateley-na-osnove-dannyh-aytrekera-tobiix2-30. Last accessed 28.12.2019
14. 15 JavaScript face detection and recognation libraries 2019, https://www.edopedia.com/blog/javascript-face-detection-and-recognition-libraries/. Last accessed 28.12.2019
15. Ethereum, https://www.ethereum.org/. Last accessed 28.12.2019
16. F. Casino, T.K. Dasaklis, C. PatsakisA systematic literature review of blockchain-based applications: current status, classification and open issues telematics Inf, 36 (2019), pp. 55-81
17. Patrick Ocheja, Brendan Flanagan, Hiroshi Ueda, Hiroaki Ogata (2019). Managing lifelong learning records through blockchain. Retrieved 2019-12-28, from https://link.springer.com/article/10.1186/s41039-019-0097-0