BLOCKCHAIN AS A SERVICE, AN APPLICATION MODEL FOR INTEGRATION OF BLOCKCHAIN INTERFACE OVER AN EXISTING SYSTEM ARCHITECTURE

V. Valkanov, M. Petrov

Abstract. Modern software architectures have to deal with challenges such as network load, scalability, availability, software and social attacks. The classic three-tier architecture model cannot offer the full range of capabilities that the business needs of applications are chasing. The ability to update the code in real-time, the connectivity of the individual components and the relationships with service providers are the main challenges that cause the need to package solutions that are provided in the form of services. In this article, we will look at the architecture of the Blockchain layer which can be integrated as an additional application to an existing database layer, in the form of an additional service to enhance the security of incoming records.

Key Words: *Blockchain, Education, Behavior tracking, distributed networks, E-learning*

Introduction

Information security is an aspect that covers all spheres of the modern industry, the transport of goods and services, the provision of medical care, and education. In the digital communications era, traditional means of obtaining educational qualifications such as Schools and Universities are increasingly giving way to alternative approaches, in the face of e-learning. Sources of information can now be found not only in the face of institutions and authorities, but increasingly in the face of professionals and professionals in the field of knowledge that are of interest to learners.

The launch and conduct of the so-called MOOC (Massive Online Open Course) [1], fully implemented with the means of modern communication

Дата на получаване: 01.11.2019 г.
Дата на рецензиране: 20.03.2020 г.
Дата на публикуване: 02.06.2020 г.

technologies, is increasingly blurring the boundaries between the classic image of universities and the classroom of the future.

Suddenly, education users find themselves at the center of a vast ecosystem of qualification courses offered by institutions of various sizes and focuses in the face of classic universities and technology platforms. Education is increasingly accessible, but the mechanisms for collecting information about the activities of students within these educational institutions are often limited to honest words and non-traceable documents [2].

The end result of the training is always a document that shows the empirical dimensions of the student's efforts, but does not give clarity on what steps he or she went through to achieve these results. Often, different institutions define speech and visual disciplines that cover virtually identical information activities in nature, but there is no mechanism through which to prove that the acquired knowledge in one direction coincides with the equivalent direction in another institution.

In practice, there is no mechanism or file of student activities that can be easily consumed regardless of the institutional model.

In the context of traditional educational institutions, departments and faculties often use a variety of information platforms to monitor student development within a course, but this monitoring is usually in isolation and ignores the student's development up to that point in his or her education. The additional knowledge is ignored and only the material concerning the current knowledge and skills of the practitioner is considered. In this way, extremely valuable information units are lost, which would not only provide an opportunity for detailed analysis to answer the question of whether the overall training course was producing the right results, but also would ignore those already accumulated.

The technology of Block-chain data storage

State of art. The term Blockchain is loosely used to describe a range of concepts that we are going to define here.

- As a data structure the blockchains is a linked list that store a number of objects connected by cryptographic data link.
- As a technology the blockchain is a decentralized distributed immutable network that allows tracing of digital transactions between users of the network.

The technology concept was promoted by Satoshi Nakamoto in 2008 [3] as a tool for realizing the Bitcoin digital currency categorized as a cryptocurrency. The concept is a direct counterpart to centralized storage and information exchange systems, which are usually private in nature, even when used for public

service needs. The technology is nowadays popular in the context of crypto currencies and the transfer of financial resources between counterparties, but the applications are practically innumerable.

An example of popular Block-chain projects is the Bitcoin network, one of the most famous examples of virtual currency. Storj decentralized cloud storage provider [12]. Neufund decentralized network for personal investment management [13].

The basic concepts that describe a blockchain storage development are:

- Immutability. Each of the entries in the chain is unique and is not subject to change [4]
- Connectability. Each of the entries in the chain is uniquely linked to the previous ones, with a hashed sequence of unique symbols to guarantee the process of tracing the connection to each other [4].
- Anonymity. Participants in the transaction process present themselves to the system through a unique sequence of randomly generated characters, often called crypto wallet. Performing a transaction and storing information is completely anonymous, thus eliminating direct tracking of a specific counterparty in the physical world [4].

The storage of information occurs in a logical unit, text file, or conventional database. Communication between different logical units is accomplished with a software tool developed for the needs of the network. A new information block is added to the chain only when the conditions of the network are fulfilled, ie agreement or consensus is reached between the participants in the network, so that the newly added information does not contradict the truth. The new block is synchronized with the network participants so that the information does not belong to one operator at a given time, eliminating the possibility of data network manipulation.

Advantages and disadvantages of using Blockchain. The main features that make the technology suitable for use and for sensitive information can be characterized as follows:

- Stable network eliminating the potential for unwanted modifications. As we said, the basic concept of a network is that it is immutable. We can rest assured that the information added to the Blockchain chain will not be changed in the future or replaced by detractors.
- Decentralization. The information is stored across multiple devices, making it secure and virtually immune to data corruption, until the system has active users [5]. The blockchain accommodate a pear to pear type of protocol, granting that the information is going to be hare between all of the participants of the communication at any time.

Of course, in its purest form, the system also has a number of shortcomings that stem from the theoretical model of decentralized and infrastructure. One of the major drawbacks comes from the block integrity validation algorithm, which, if not properly selected, can lead to significant performance degradation of the whole system [6]. Also, if the correct model for compression of the input data is not selected, the cluster of information may become too large to be adequately distributed among all users on the network. The solutions to these problems will be discussed in the next chapter of the article, but overall, they depend on the specific implementation of the system that utilizes the Blockchain concept.

Integration of Blockchain technologies in education

Learning is an incremental process, it begins and ends with human life, formally, classical education can give basic knowledge and skills that people develop by accumulating professional experience and upgrading their skills through attending various courses, seminars conferences, as well as through increase their professional experience practical experience and theoretical background.

In order to deliver this training, e-learning systems typically use e-learning access systems that provide a mechanism for interacting with the study material, solving tests, communicating with teaching staff, and obtaining a specific document that guarantees the outcome of that training [7].

On the territory of the university the concept is similar, each of the students depending on their specialty attends a training course that aims to broaden their knowledge. In order to receive adequate information from this course, students study additional materials from external sources, as well as use popular platforms for acquiring additional knowledge and skills, such as YouTube[14], Khan Academy[15], Coursera and others. Completing a course carries with it an assessment, but excludes activities that can be finely analyzed.

For example, teaching a mathematical discipline requires the acquisition of a complex set of knowledge and skills, the final exam carries an empirical grade of 2 to 6, but this assessment does not give semantic information to the next teacher who aims to develop the student's skills by showing him or her additional materials to build on the knowledge he has acquired, or by trying to fill specific gaps.

At the same time, teachers remain unaware of the additional activities of students in the online space, which may provide additional light for attempts to develop the potential in a given direction. For this reason, there is a need to have a mechanism in place to fully monitor student behavior between seemingly unconnected platforms.

Integration of private Blockchain with existing educational platforms

Existing independent educational platforms. A variety of internal student preparation and training systems operate at the University of Plovdiv. Examples of such systems are DELC1, DECL2, UniPlayground, their purpose is to support the learning process by utilizing the training tools needed and aggregating additional information providing a wide range of the possibilities of the teaching staff. For additional preparation, students most commonly use platforms such as Khan Academy to further improve their knowledge in Mathematics, Coursera for a variety of computer science courses, such as Artificial Intelligence, Introduction to Computer Science, Discrete Mathematics, Data Structures and Algorithms. The systems listed have self-contained modules to keep track of student development, such modules are:

- Modules for solving test tasks, for intermediate and final evaluation
- Tracking system activity, reading articles, or checking homework.
- Modules for reporting end activity, such as end value or end point asset
- Feedback modules from a teacher, colleague or student
- Modules for implementation and monitoring of team activities, group projects or supervision

All these additional systems make it possible for students to improve their preparation, but the most important point is that they generate information, which quite often remains only within the system [8].

There is an indirect link between social networks and platforms, such as Coursera and Khan Academy, allowing the completion of a course to be tracked by providing a public link to access the platform and visualize information in the form of a certificate. This activity is carried out at the request of the participants in the program, and they have the opportunity to share all the information about their activity in the system.

UniChain private distributed blockchain platform. In order to make the connection between the different systems, it is necessary to introduce an additional intermediate layer to aggregate and record information about the activities of students in the different platforms. This task is performed by an independent platform, UniChain, a decentralized cloud system, for managing the flow of resources between unconnected systems [9]. It is an anonymous, decentralized, system that stores a set of meta information regarding events occurring in educational systems. The events that have occurred are recorded, shared voluntarily by the participants in the courses and provide additional information to the consumers in the other courses.

UniChain is a decentralized sequence of logical blocks containing a timer and a collection of data that are linked together by a cryptographic identifier that uniquely indicates the direction between two linked blocks. The information that can be stored in each of the blocks is divided into the following categories

- Information on the intermediate result achieved
- Outcome information
- Meta information regarding an intermediate event

Let’s look at the three aspects in more detail. Intermediate result information is any result of an intermediate exam, or a final exam that accumulates any grade, the information about that result is processed by the system along with additional information about the activities that suggest that result.

At this stage, each block consists of the following identifiers

- The name of the discipline, the course
- Information on the subject on which the exam topic is administered
- Information about the exam material
- The end results

The end result information includes the accumulated number of points or an empirical evaluation of the activities carried out so far, as well as verification of the certificate or diploma obtained from the accrediting platform, the student's results.

Intermediate status meta information is an undefined and general area that makes it possible to record any important information resource, such as achieving consistent reading of a certain type of information, or attending classes regularly.

This is a category of information that is specific to each individual platform and can support the student's overall information file depending on his or her activities.

Let's look at an example, for additional information that does not strictly address student achievement and attainment. There is an integrated classroom access system on campus, in which students can be verified with magnetic cards or fingerprints, information is stored in the campus-operated system, and the arrival of study time is meta information that can be synchronized with the blockchain and demonstrate active presence within the classroom.

Unichain architecture

Establishing active network communication, activity and wallet. To become part of the system, the user downloads a software portfolio provided by

the educational institution. The portfolio plays the role of a mediator between the platforms the client visits and the UniChain network. At its core, the portfolio is a client built as a mobile or desktop application that has implemented interfaces to access the platforms that students visit.

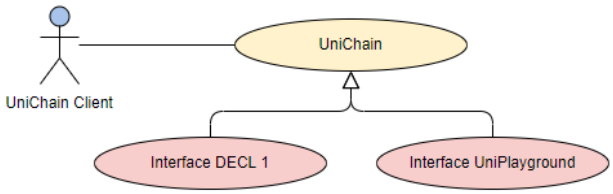

Figure 1. Interfacing blockchain with external platforms and communication agents

Users who are successfully logged into the UniChain system create a unique identifier for their activity and agree to share information from platforms that are integrated with the network.

Communication interfaces. Communication between the various system components is based on interfaces. UniChain implements access to user information stored in the designated information resource flooding system and actively communicates when an event occurs. Event synchronization occurs either explicitly at the request of clients or with active communication between the system and the UniChain network.

UniChain is a blockchain application based on the Service oriented architecture model [11]. The main objective is to provide a set of services that can allow other connected systems to receive information from the network, with the express permission of the user. The active communication process enables integration with a new system to access information about all activities within existing systems. The interface allows users to categorize their activities without allowing them to modify the data.

Storage of resources. A major problem with blockchain technologies is their scalability. Due to their decentralization, it is necessary to keep the files and information of the users consistent within the active devices. This often takes a huge amount of resources at a time when the network is gaining enough popularity. The storage of a 1MB file soon generates a huge amount of data that is stored within the active blocks. Such information may be a file, certificate, or other voluminous information.

UniChain solves the problem by keeping the files separate from their signature. The file storage signature is a cryptographically hashed meta data set indicating the file resource path stored on simple storage containers optimized for file resource storage. Only the identifiers that are being checked are matched to the active blocks on the chain blocks. The files containing the real resource are stored in a decentralized manner in an optimized cloud-based storage provider network. If an event occurs that invalidates the files, then their cryptographic

signature will be compromised and no direct connection will be found between the replaced file and the recorded signature on the blockchain network.

Detection of inconsistency in the recorded information (consensus algorithm). The blockchain loses its reliability when the data in it is commented on, so it is necessary to check to what extent the records in the individual blocks are positioned valid throughout the network while the distribution process is in progress. Conceptually the most popular verification algorithm is the Proof of work used on the Bitcoin network, but one of the major drawbacks is the concept of engaging resources competitively to be rewarded through some resource.

The UniChain Network does not provide a prize pool, so active resources will be verified for active parties using the Proof of Authority algorithm. The concept behind this mechanism is that a small number of network members are authorized to verify the availability of an update, synchronizing blocks with all actors in the chain. Unlike the classic model, these participants will not be permanently involved in the process but will be selected at random depending on their activity. One of the private platforms selected at random will always be involved in the verification of the data.

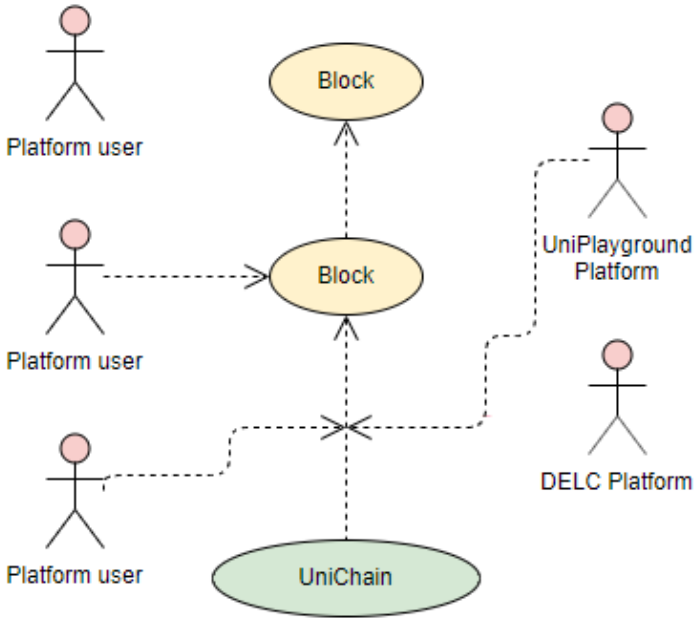

Figure 2. Choosing a random user and platform for proving the validity of the block-chain

Problems, goals and further development of the prototype

The Blochain technology is not just a hype inflated by the media it is a promising technology that can benefit the development of storage related application that demand high level of reliability. The presented prototype is a work in progress application system that set for itself two major goals.

At one hand to integrate and analyses the potential application of blockchain concepts for the needs of the university infrastructure.

On the other hands to practically test and expand the already established concepts by actively improving the existing concepts.

The projects is going to integrate with a number of different application platform and practically test the reliability of the concepts.

Conclusion

In this article, the architecture and main components of a private network for storing student achievement information in the context of their e-learning were presented. The technology of the application is based on the concept of storage of information in the model of a block chain guaranteeing immutability and decentralization of the stored data, for the purpose of high level of security and prevention of malicious manifestations.

The project aims to provide up-to-date information on the results achieved in arbitrary educational institutions guaranteeing transparency and an additional level of analysis in the provision of a quality information product to higher education trainers [12]. The proposed model can also be integrated into other areas of public e-learning, changes related to such implementation depend on the model of access to the system and the characteristics of the stored information.

The proposed approach for integrating systems based on interfaces guarantees the possibility for the participants in the system to guarantee their activity at any moment without compromising the activity of the network. We intend to complete all of the tasks and extend the concepts in the near future.

Acknowledgments

The paper is co-funded by the Project FP19-FMI-002 “Innovative ICT for Digital Research Area in Mathematics, Informatics, and Pedagogy of Education” of the Scientific Fund of the University of Plovdiv Paisii Hilendarski, Bulgaria.

References

[1] Hollands F. Tirthali D. MOOCs: Expectations and Reality Full Report (May 2014)

[2] Bartolome A. Blockchain in education. Introduction and critical review of the state of the art (November 2017) ISSN 1135-9250

[3] Nakamoto, S. (31 October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System

[4] Science, G. O. for. (2016). Distributed Ledger Technology: beyond block chain.

[5] Daniel Drescher Blockchain Basics: A Non-Technical Introduction in 25 Steps. ISBN-13: 978-1484226032

[6] Bauerle, N. (2017). What is the Difference Between Public and Permissioned Blockchains? Retrieved March 10, 2018, from https://www.coindesk.com/information/what-is-the-differencebetween-open-and-permissioned-blockchains/

[7] Blockcerts. (2016). Blockcerts. The open standard for blockchain credentials. Retrieved August 20, 2003, from https://www.blockcerts.org/

[8] Bore, N., Karumba, S., Mutahi, J., Darnell, S. S., Wayua, C., & Weldemariam, K. (2017). Towards Blockchain-enabled School Information Hub. Proceedings of the Ninth International Conference on Information and Communication Technologies and Development - ICTD '17, 1–4. https://doi.org/10.1145/3136560.3136584

[9] Chen, G., Xu, B., Lu, M., & Chen, N.-S. (2018). Exploring blockchain technology and its potential applications for education. Smart Learning Environments, 5(1), 1. https://doi.org/10.1186/s40561-017-0050-x

[10] Rooksby, J., & Dimitrov, K. (2017). Trustless Education? A Blockchain System for University Grades. New Value Transactions Understanding and Designing for Distributed Autonomous Organisations Workshop at DIS 2017, (June 2017).

[11] Siau K. Service oriented architecture: A research review from the software and applications perspective

[12] Skiba, D. J. (2017). The Potential of Blockchain in Education and Health Care. Nursing Education Perspectives, 38(4), 220–221. https://doi.org/10.1097/01.NEP.0000000000000190

[13] Storj (https://storj.io/)

[14] Neufund (https://neufund.org/)

[15] YouTube (https://www.youtube.com/)

[16] Khan Academy (https://www.khanacademy.org/)

Faculty of Mathematics and Informatics,

University of Plovdiv "Paisii Hilendarski",

24 Tzar Asen Str., 4000 Plovdiv, Bulgaria,

E-mails: vvalkanov@uni-plovdiv.net, mail@mihail-petrov.me

ИНТЕГРАЦИЯ НА БЛОКОВИ ВЕРИГИ, ПОД ФОРМАТА НА ВЪНШНИ УСЛУГИ, В СЪЩЕСТВУВАЩИ СИСТЕМНИ АРХИТЕКТУРИ

В. Валканов, М. Петров

Резюме: Съвременните софтуерни архитектури трябва да се справят с актуални предизвикателства на потребителското поведение като натоварване на мрежата, мащабируемост, постоянно наличност, софтуерни и социално инженерни атаки. Класическият трислоен архитектурен модел не може да предложи пълния набор от възможности, които бизнес изискванията на приложенията са длъжни да предоставят. Възможността за актуализиране на кода в реално време, свързаността на отделните компоненти и връзките с доставчиците на услуги, са основните предизвикателства, които предизвикват необходимостта от предоставяне на решения, които се предлагат под формата на услуги. В тази статия ще разгледаме архитектурата на така наречения слой на блоковите вериги, който може да бъде интегриран като допълнително приложение към съществуващ слой база данни под формата на допълнителна услуга за повишаване на сигурността на входящите записи.

Ключови думи: *блокови вериги, образование, проследяване на поведението, разпределени мрежи, електронно обучение*