Journal of Physics: Conference Series

PAPER • OPEN ACCESS

The implementation of Blockchain framework in MOOCs to support a freedom of learning in Indonesia

To cite this article: F G Febrinanto *et al* 2021 *J. Phys.: Conf. Ser.* **1836** 012043

The implementation of Blockchain framework in MOOCs to support a freedom of learning in Indonesia

F G Febrinanto[1], Dafik[2,3], and R Nisviasari[3]

[1]Federation University, Ballarat, Australia
[2]Department of Mathematics Education, Universitas Jember, Indonesia
[3]CGANT Research Group, Universitas Jember, Indonesia

E-mail: falihgozifebrinanto@students.federation.edu.au; d.dafik@unej.ac.id

Abstract. A freedom of learning program has been released by the Indonesian Ministry and Culture this year 2020. There are three ways for students to earn their credits, namely take the subject course in face-to-face based class, virtual based class or under Massive Open Online Courses (MOOCs). MOOCs is a model that is developed to help people to learn about certain skills through the online platform, without any limitation in the audience. MOOCs aim to enhance broad collaboration between individuals in creating learning environments that have high scalability and can be accessed by anyone and anywhere. The complexity arises when students undertake a subject course through MOOCs, how to certify the completion of their program in which the certification can be gained easily, and the last how secure the obtained certificate? Blockchain technology can help to improve the quality of MOOCs by providing control of academic records as evidence that someone has completed a learning process on MOOCs. Academic records generated will be stored in one place forever and safely stored in the Blockchain environment. This article will explore how the possible to implement the Blockchain framework in MOOCs to support a freedom of learning in Indonesia.

1. Introduction

Education is a worthwhile investment for individuals to increase their quality of life in the fields of economics and social. Higher education guarantees long-term economic benefits to whoever does it, see Pouezevara et al. [5]. Moreover, education can enhance one's knowledge to become a professional in specific sectors in their life. To get new skills and insights, people can participate in a learning program provided by educational institutions such as universities or schools. Students are required to come to the universities or schools following the learning process, doing the assignments, and taking the exams to fulfill the prerequisite of graduation established by the educational institutions

Nowadays, with the innovation of technology in the field of education, especially in the freedom of learning program endorsed by by the Indonesian Ministry and Culture 2020 [3], students can take online courses via the internet, more specifically through Learning Management System (LMS) platform. This type of learning process is considered to be online courses. There are many advantages of online course program, one of those is the absence of students coming to school classroom. They can joint the class anytime, anywhere and anyplace. It would be a great opportunity for students who want to get an education but unable to join the offline class. Currently, there is a new model of learning management system called Massive Open Online Courses (MOOCs). MOOCs have many benefits compared to the traditional online class, for example, it is opened for all components of the society, and it has no limitation of numbers of the audience. Furthermore, the audiences are free to choose their learning schedule, anytime and anywhere, Khadiri et al. [4]. MOOCs also provide many options for courses that can be engaged in the student's interest.

Besides the advantages of MOOCs, acceptance of the MOOCs certificate, gotten after course completion, is required to be verified and validated. In this research, we identified several problems that must be solved to improve the quality of recognition of the certificates. The first problem is how to save certificate documents in long-lived storage. Secondly, to avoid a forgery certificate becomes more prevalent due to the ease of the use of software editing. When it is happened, it is difficult to distinguish between the original and the fake one. Without a reliable verification process on the certificate, unauthorized parties can be easily manipulated existing documents. Third, the other essential elements to pay attention are recognition, accessibility, and trustworthiness. Recognition means how stakeholders or institutions can easily recognize the original certificates. Next, accessibility means how stakeholders or institutions able to access certificates obtained by students. Last, trustworthiness is also an important point on certificates because it shows how much people trust the authenticity of the certificate.

There is a promising technology called Blockchain that can store data in a clear and tamper-resistant manner which is implemented in a distributed network. When we talk about Blockchain, this technology reflects digital information stored in public databases, refers to Yaga et al. [11]. The hope is that Blockchain technology will be implemented in MOOCs so that certificates issued can be officially published and recognized and can also be stored permanently and cannot be deleted. With these problems and opportunities, we initiated a review of Blockchain technology so that it can be used to improve the quality of online certificates. Furthermore, since we implement the blockchain technology we need a secure management key to encrypt and decrypt the secret sharing key. For this purpose, we will use a labeling key, namely super *(a,d)-H* antimagic total labeling of graph. This article, we will explain the framework for implementing Blockchain technology in issuing certificates for MOOCs.

2. Literature Review

2.1 MOOCs

MOOCs (Massive Open Online Courses) are a disruptive technology of new online learning which has more advantages over traditional online courses. The advantages of MOOCs that are different from traditional online courses such as open to all components of people, have no limit on the number of students and can be accessed anytime / anywhere without any limits, see Pouezevara et al. [5].

MOOCs have four main components: Massive, Open, Online, and Course. Massive can be interpreted as providing accessible learning platforms to a large number of students who want learning at the same time. Open means that registration can be done by anyone, anywhere, and anytime without limitation. The online component means that the courses are taken entirely online via the internet. The last component is a course that has the same meaning as the courses in higher education, but it does not offer credit points.

2.2 Blockchain

Blockchain technology is a series of databases containing records of transactions. Blockchain technology has a distributed concept on computer networks to validate existing data. Unlike traditional databases, information on the blockchain cannot be manipulated because the model is built on a distributed nature and confirmed with guarantees by each peer/node. In a blockchain network, all nodes can access information from each other so that there is no central entity control. This concept makes blockchain technology different from the traditional database which has access to a single point/or several determined points, Sarmah [8]. In Figure 1 we can see the example of blockchain structure.

Based on figure 1, when someone makes a transaction on the blockchain network, to enter the existing chain, the transaction will be verified and validated using a computer algorithm to determine the authenticity of the data. Each block has a header and a series of transactions. The header contains link pointers to indicate the previous block and the next block. Moreover, the header also contains information about a timestamp so that the tracing process can be carried out to get the chronological order on the blockchain. Blockchain technology also relies on hash technology to ensure the data on the block cannot be tampered with or altered, Wang et. al [10].

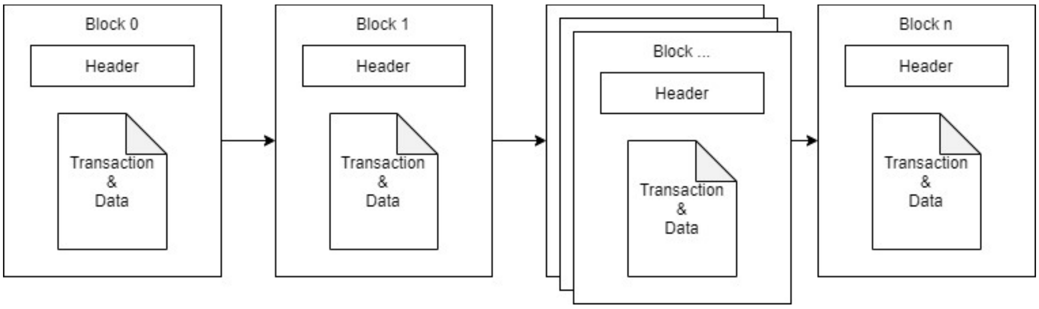

Figure 1. Blockchain structure.

2.3 Transaction and data

In the blockchain component, there is a transaction which is defined as the smallest unit stored on public records. On a transaction blockchain, there is a component called a data field that can be filled with any data that the sender wants. The data in the transaction can be compiled in JSON format then the format is converted into hexadecimal for the encoding process. The encoded data is entered in the data field of a blockchain transaction, Wang et. al [10]. The execution of transaction records on the blockchain requires validation by all nodes joined to the blockchain network. Previous transaction records can be checked or re-validated but cannot be deleted or updated by further steps Sabry et al. [7].

2.4 Smart contract

A smart contract is a protocol that governs the blockchain platform which is based on an automated process. Smart contracts legally control documents are based on actions or events that have been approved based on the contract and agreement, read Savelyev [9]. Implementing a smart contract in order to comply with the self-executive principle, all entities and nodes must be involved to implement the smart contract that has been determined through the lines of program code Zhou et al. [12].

2.5 Decentralized Ledger

A decentralized ledger is a database that is synchronized on all nodes in a network. A decentralized ledger can also be called a shared and replicated database that stores transactional data for all members in the network, see Sarmah [8]. The decentralized ledger also eliminates the central authority to maximize the checking process of data manipulation. All data or information on the decentralized ledger is stored safely and accurately using cryptographic methods. Data and information can only be accessed using correct cryptographic keys and signatures. After the data is successfully stored, it will be available permanently and cannot be deleted according to the rules on the blockchain network.

2.5 The $(a, d) - H$antimagic total labelling

Given that a simple, and undirected graph G. By H antimagic total labeling, we mean an assignment of integers to the either vertices or edges of G such that every evaluation of element sub graph H shows the different weight, see [2]. It is said to be super if the smallest elements appear on the label of vertices.

3. Research methodology

Research methodology explains the steps that will be conducted in qualitative research for making a framework of blockchain technology. The steps of research methodology can be seen in Figure 2 below:

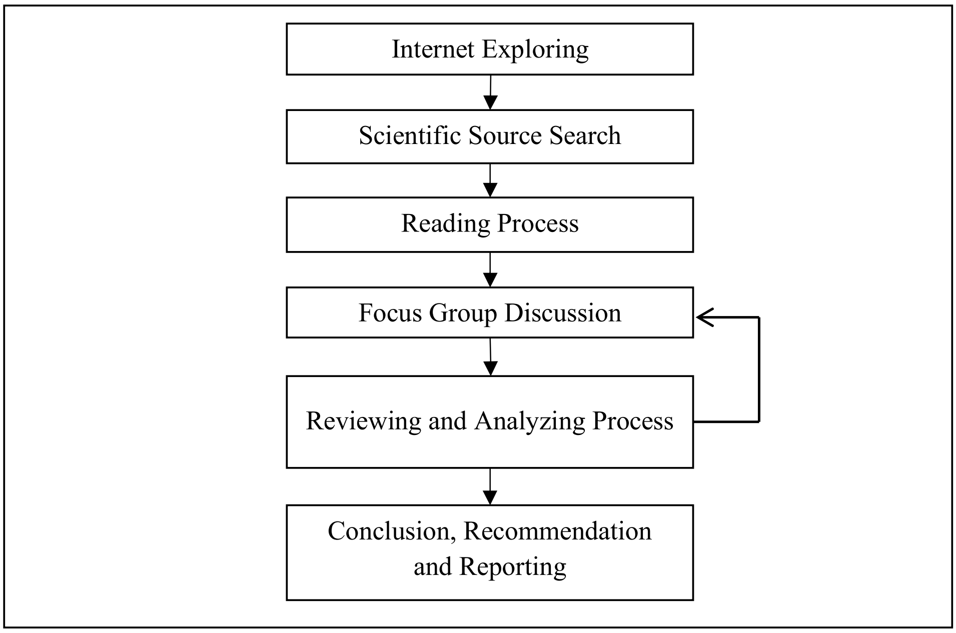

Figure 2. The steps of research methodology.

3.1 Internet Exploring

At the beginning of this research, exploring the internet was conducted to gain information about the enormous use of technology for education and training. Nowadays, we know that many online platforms were developed to deliver courses without any limitation of audiences. From this information, potential issues related to the massive use of open online platform were acquired. It leads the researchers to get the topic of this research.

3.2 Scientific Source Search

A scientific source search proposed to discover new information through study literature that systematically planned to gather important and relevant data. The researchers learn about the concept of blockchain technology and gain knowledge about MOOCs (Massive Open Online Courses) include its benefits and issues. One of those issues is about recognition of MOOCs certificate earned after completion.

3.3 Reading Process

Reading process aimed to understand the relation of every evidence of selected issue with the use of MOOC. This process also contains of issues breakdown which divide into five main points: retention, forgery avoidance, recognition, accessibility, and trustworthy.

3.4 Focus Group Discussion

Focus group discussion is gathering a group of people who have an idea to implement the blockchain technology in MOOCs system as a form of qualitative research. The group will be discussing about the problem related to MOOCs. They could share their perceptions, opinion, or ideas. The goal of this activity is to find the most suitable solution of MOOC certificate problem without decrease the value.

3.5 Reviewing and Analyzing Process

At the end of this research, the result of focus discussion group will be analyzed and examined to obtain needed framework to implement blockchain technology in issuing the certificate of MOOCs. In this research we try to make framework for the blockchain technology that has contribution to eliminate case of certificate forgery.

3.6 Recommendation

The last step will be carried out after all the stages have been completed from the planning stage to the testing stage by making a final conclusion. Apart from that, the final step also includes suggestions after doing this research. The function of the recommendations is to provide suggestions for future research to improve the findings.

4. Blockchain for Improving MOOCS

In this section, we will discuss how blockchain can be used in issuing certificates for MOOCs. Blockchain is expected to be able to minimize the problems and improve the quality of the course certificates issued by MOOCs providers. With a distributed database and a validation system that is supported by a smart contract, it will help to save documents in long-life storage and also avoid document forgery. The anytime-access blockchain network and validation process using the cryptographic method will help to improve the three important elements of a certificate, namely recognition, accessibility, and trustworthiness. Moreover, information can only be accessed using correct cryptographic keys and signatures. Eventually, it will increase user confidence and trust because it has been checked by a reliable system.

Frameworks for implementing blockchain technology on the MOOCs system. Two frameworks will be discussed in this section. The first framework is a framework for issuing certificates from MOOCs providers to students who pass certain courses. The second framework is a framework that is used for conducting a certificate checking process which is useful for checking the authenticity of certificates whose information is needed by other stakeholders or institutions. Figure 3 below describes the framework for the issuing certificate process on the blockchain network.

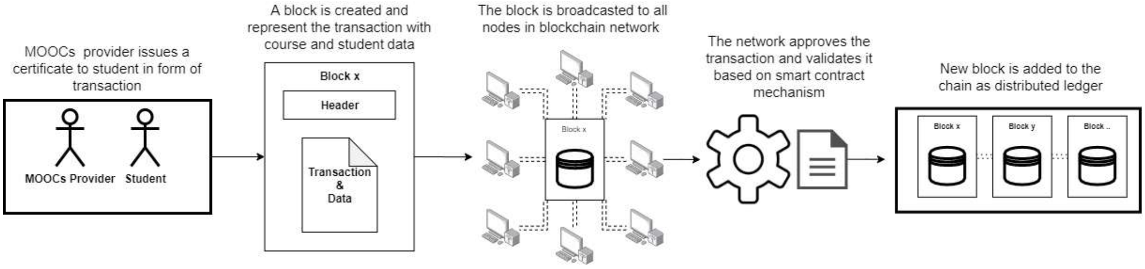
MOOCs provider issues a certificate to student in form of transaction
MOOCs Provider
Student
A block is created and represent the transaction with course and student data
Block x
Header
Transaction & Data
The block is broadcasted to all nodes in blockchain network
Block x
The network approves the transaction and validates it based on smart contract mechanism
New block is added to the chain as distributed ledger
Block x
Block y
Block ..

Figure 3. Framework for issuing a certificate process.

Figure 3 describes the process of issuing a certificate that begins with the initiation of the MOOCs provider. After finishing the course, The MOOCSs provides a certificate to the student. The MOOCs provider issues a certificate in the form of a transaction in the blockchain network. Then a block that represents a transaction with the course and student data will be created. The block is then broadcasted to all nodes in the blockchain network to implement the distributed ledger concept. The block will be synchronized across all nodes in a network. Each node on the network then carries out approval and validation based on the smart contract that has been created. The smart contract will automate the validation process on the newly created block. When the validation process is accepted, the block will be added to the existing distributed ledger which forms a chain that provides a transparent and permanent record of data. After the process is complete, the student legally receives a certificate that has been issued by the MOOCs provider. This concept is believed to improve the quality of existing certificates because it has been done through a sophisticated verification process.

Not only is the issuing certificate process by MOOCs providers important in implementing blockchain technology but also how the institution or stakeholder can also check the authenticity of the certificate. Figure 4 describes the framework for checking the authenticity of certificates.

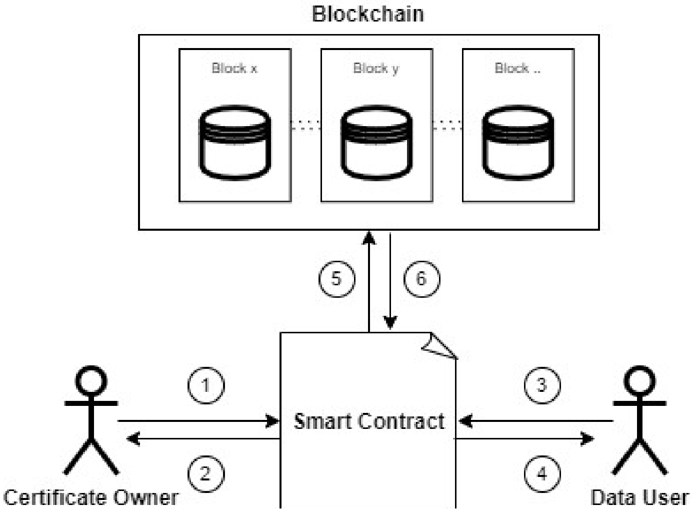

Figure 4. Framework for checking a certificate.

In Figure 4, there are two main actors: the certificate owner and the data user. The certificate owner is a student who has passed a certain course and who received the certificate. The data user is an actor who will use certificate data, it can be stakeholders or external institutions. Data user requires information about the authenticity of certificates for any event or process in their organization. The blockchain network stores existing certificate data so that each actor can reliably check existing data on the blockchain network. The description related to the framework in Figure 4 can be seen in the explanation below:

Framework 1. The integration process of blockchain into MOOCs.

1. Certificate owners can access their encrypted data by providing a secret key in which the decryption process is managed by the smart contract.
2. Certificate owners get the decryption of their data stored on the blockchain with the help of the smart contract mechanism.
3. User data can access certificate data by providing a shared key to check the authenticity of the certificate.
4. User data gets feedback about the authenticity of the certificate.
5. Smart contracts access data on the public ledger to obtain information based on the key provided by the user.
6. Smart contracts get information about existing data from the blockchain network to be given to users.

With this process, the validation or checking certificate process becomes more reliable and it can minimize data falsification. Eventually, the implementation of blockchain technology in the MOOCs system can improve the quality of the certificates issued by the MOOCs provider.Furthermore, how to develop the secure encryption and decryption data mentioned in above framework, we will use a Cipher Block Chaining (CBC) and also integrate the super $(a,d)-H$ antimagic total labeling of graph in the CBC algorithm.

5. Encryption process by using graph labelling for the key

By the Framework 1, we can see blockchain technology relies on the management key to secure the certificate document gained from MOOCs in. Thus, when we need to store the certificate, firstly, we need a secret key such that it is difficult for any hacker to decrypt the data. We will use graph labelling for developing the secret key. The existing algorithm to establish a stream cipher under the mode of Cipher Block Chaining, we guide the reader to a published paper in [6]. We give an illustration of graph labelling of super $(a, d) - H$ −antimagic total labelling of graph $shack(H, v, n)$ to construct the encryption keys. Take a super (1351,39)-$P_2 \rhd W_5$-antimagic total labelling of graph $G = C_5 \rhd W_5$ obtained in [1]. An established algorithm stated in [6] regarded to the development of stream cipher of Cipher Block Chaining by implementing the above super (a, d)-H antimagic total labelling of graph G, see Figure 5 and Figure 6 for detail illustration.

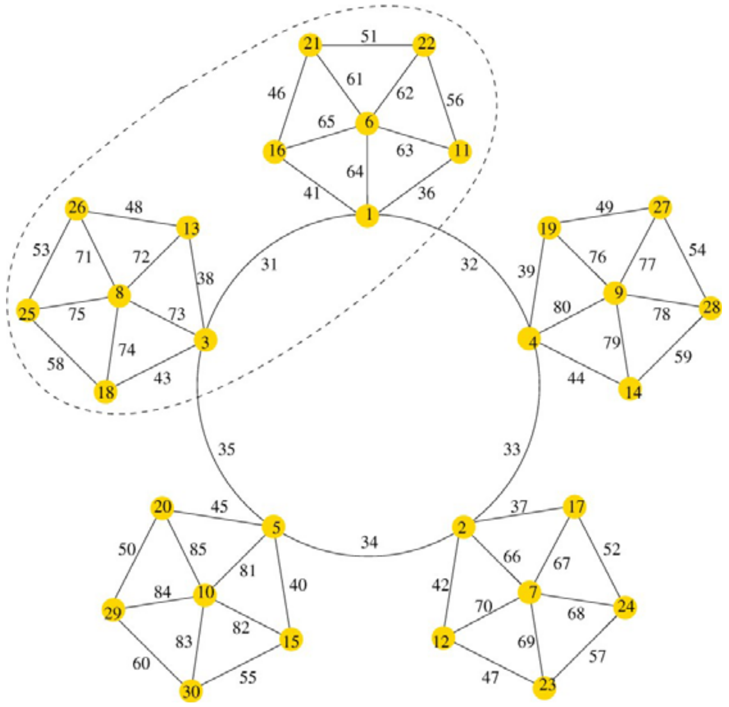

Figure 5. Super (1351,39)-$P_2 \rhd W_5$-antimagic total covering of graph $G = C_5 \rhd W_5$.

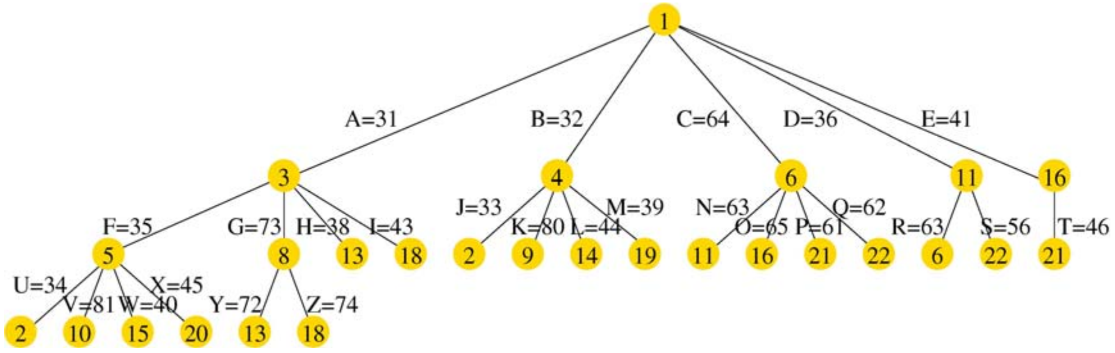

Figure 6. The layered diagram of super (1351,39)-$P_2 \rhd W_5$-antimagic total labeling of graph $G = C_5 \rhd W_5$.

The source key obtained from a layered diagram, see Figure 6, are 31, 32, 64, 36, 41, 35, 73, 38, 43, 33, 80, 44, 39, 63, 65, 61, 62, 63, 56, 46, 34, 81, 40, 45, 72, 74. In modulo 26, they are 5, 6, 12, 10, 15, 9, 21, 12, 17, 7, 2, 18, 13, 11, 13, 9, 10, 11, 4, 20, 8, 3, 14, 19, 20, 22. Suppose the length of block is given by 3. We have the stream function is $k_{j+3} = k_j + k_{j+1} mod\ 26$. The initial block key is $k = 5, 6, 12$ and the key stream is (5, 6, 12), (11, 18, 22), (25, 24, 4), (7, 3, 24), (9, 20, 5), (24, 24, 22), (19, 21, 15), ... Table 1 show how the key stream obtained from the algorithm to establish the stream cipher in the mode of Cipher Block Chaining by using super (1351,39)-$P_2 \rhd W_5$-antimagic total labeling of graph $G = C_5 \rhd W_5$.

Furthermore, how does it work for the certificate completion document of MOOCs? We will give the following illustration in Table 1.Given that someone has finished on a specific course in MOOCs, namely "COMBINATORIALMATHSPYM". We consider the text COMBINATORIAL MATHS PYM" consist of the name of subject course is Combinatorial Mathematics, and the lecturer is Prof. Yung Ma (PYM), it is available in the *Edx* MOOCS. He has passed and gained a certificate. The smart contract developed the secret key by using graph and by means of Cipher Block Chaining. The smart contract can generate the ciphertext of "COMBINATORIALMATHSPYM" such that anyone will access the certificate, either the certificate owner and the data user can access through the the chipertext. For the detail how to encrypt the name of subject course and the name of the lecture who teach this course, it can be describe the following table.

The smart contract develop the secret key by mean of super *(a,d)-H* antimagic total labeling elements in Table 1. By mean of CBC, the encryption key as a chipper text is HUYTUHSLZQWXKCCBHQJAR. Certainly, this ciphertext is hard to reveal by any intruder or an authorised person. By doing the reverse the CBC algorithm we can have the plaintext again.

Table 1. The encryption process.

Plaintext	C	O	M	B	I	N	A	T	O	R	I	A
P_i	2	14	12	1	8	13	0	19	14	17	8	0
C_{i-1}	0	0	0	7	20	24	19	20	7	18	11	25
P_i'	2	14	12	8	28	37	19	39	21	35	19	25
K_i	5	6	12	11	18	22	25	24	4	7	3	24
C_i	7	20	24	19	20	7	18	11	25	16	22	23
Ciphertext	H	U	Y	T	U	H	S	L	Z	Q	W	X
Plaintext	L	M	A	T	H	S	P	Y	M			
P_i	11	12	0	19	7	18	15	24	12			
C_{i-1}	16	22	23	10	2	2	1	7	16			
P_i'	27	34	23	29	9	20	16	31	28			
K_i	9	20	5	24	24	22	19	21	15			
C_i	10	2	2	1	7	16	9	0	17			
Ciphertext	K	C	C	B	H	Q	J	A	R			

Table 2. The decryption process.

Ciphertext	H	U	Y	T	U	H	S	L	Z	Q	W	X
C_i	7	20	24	19	20	7	18	11	25	16	22	23
C_{i-1}	0	0	0	7	20	24	19	20	7	18	11	25
P_i'	7	20	24	12	0	-17	-1	-9	18	-2	11	-2
K_i	5	6	12	11	18	22	25	24	4	7	3	24
P_i	2	14	12	1	8	13	0	19	14	17	8	0
Plaintext	C	O	M	B	I	N	A	T	O	R	I	A
Ciphertext	K	C	C	B	H	Q	J	A	R			
C_i	10	2	2	1	7	16	9	0	17			
C_{i-1}	16	22	23	10	2	2	1	7	16			
P_i'	-6	-20	-21	-9	5	14	8	-7	1			
K_i	9	20	5	24	24	22	19	21	15			
P_i	11	12	0	19	7	18	15	24	12			
Plaintext	L	M	A	T	H	S	P	Y	M			

6. Conclusion

Blockchain is a new concept that offers many opportunities to solve problems related to transactional data. By implementing blockchain on issuing certificates on MOOCs, hopefully, it can solve problems such as storing documents in long-life storage, avoiding the document forgery, making it easy to access the MOOCs certificate, and improving trust or reliability from user data. The proposed framework is expected to be used as a reference for implementing blockchain technology on the MOOCs system. The future of blockchain technology is very promising, so further research is needed to discuss the existing challenges to maximize the effectiveness of using blockchain technology. Eventually, we expect that blockchain technology is not only used for successful implementations of financial technology or crypto currency but also is used to store other valuable assets. More specific case, respecting to the implementation of MOOCs together with a complex cryptosystem by using graph labelling can be integrated in learning management system such as MOOCs to support a freedom of learning program in Indonesia, to have a better quality of education.

Acknowledgment

Herewith, I deeply acknowledge to CGANT-RG, the University of Jember Indonesia, for the support of this research activity for the year 2021.

References

[1] Agustin I H, Prihandini R M, and Dafik 2019 $\boldsymbol{P_2} \rhd \boldsymbol{H}$-super antimagic total labeling of comb product of graphs *AKCE International Journal of Graphs and Combinatorics* **16** 163-171

[2] Gallian, J A 2019 A dynamic Survey of Graph Labeling *The Electronic Journal of Combinatorics* 1-553

[3] Junaidi A et al. 2020 The Guideline of Curriculum Reconstruction of Higher Education in the Era of industry 4.0 to Support the Program of Freedom of Learning and the Freedom University untuk mendukung merdeka belajar-kampus merdeka, Direktorat Jenderal Pendidikan Tinggi. Kemendikbud, Jakarta, Indonesia.

[4] Khadiri K E, Labouidya O, Kamoun N E, and Rachid H 2019 Success factors in a mooc massive device: Questions and challenges *Journal of Theoretical and Applied Information Technology* 1167-1178.

[5] Pouezevara S R and Horn L J 2016 MOOCs and Online Education: Exploring the Potential for International Educational Development *RTI Press Publication* 1-11 (Research Triangle Park: RTI Press)

[6] Prihandoko A C, Dafik, and Agustin I H 2019 Implementation of super H-antimagic total graph on establishing stream cipher *Indonesian Journal of Combinatorics* **3**(1) 14-23

[7] Sabry S S, Kaittan N M, and Ali I M 2019 The road to the blockchain technology: Concept and types *Periodicals of Engineering and Natural Sciences* **7**(4) 1821-1832

[8] Sarmah S S 2018 Understanding Blockchain Technology *Computer Science and Engineering* **8**(2) 23-29

[9] Savelyev A 2016 Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law *Higher School of Economics Research Paper*

[10] Wang S, Zhang Y, and Zhang Y 2018 A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems *IEEE Access* **6** 38437-38450

[11] Yaga D, Mell P, Roby N, Scarfone, and Karen 2018 Blockchain Technology Overview *National Institute of Standards and Technology Internal Report 8202* **66**

[12] Zhou I, Makhdoom I, Abolhasan M, Lipman J, Shariati, and Negin 2019 A Blockchain-based File-sharing System for Academic Paper Review *Conference: International Conferences on Signal Processing and Communication Systems* 1-10 (Gold Coast: IEEE)