Blockchain Technology Application: Authentication System in Digital Education

Amitkumar[1], M. Ifran Sanni[2], Dwi Apriliasari[3]
[1]Veer Narmad South Gujarat University, India
[2,3]University of Raharja, Indonesia
e-mail: amit000790@gmail.com[1], ifran@raharja.info[2], dwi.apriliasari@raharja.info[3]

Abstract

The application of technology in various aspects of life has made it easy for many people. However, there are also shortcomings in the use of technology, one of which is security issues, both transactions and data. Given these issues in this paper, we propose blockchain technology for an authentication system that will protect data rights and interests and be safe from interference to store information in the form of confidential text, especially in the application of technology in education. From this writing, there are 2 benefits, the first is that all data stored in the education system is guaranteed and there will be increased trust from both parents, teachers and other parties due to the decentralized nature of blockchain.
Keywords: *Authentication, Digital Education, Blockchain, Technology.*

1. Introduction

The development of information technology is progressing very rapidly, computers as electronic data processing media can present various information and data processing quickly, precisely and accurately [41] [46]. The "Internet"-related policy has been issued since 2015 by the State Council to explore the latest models in educational services and encourage education [36] and IT companies to develop online education services[1] [43]. However, there are serious problems [44], such as the unguarded rights and interests of the owner's data, the easy distribution of data, and the illegal misuse of the transaction process. Some of these problems have triggered disputes in the development of online education services developed by education companies and IT companies. Security is one of the most important concerns in industry 4.0 [47], given that vulnerabilities that arise during production (e.g. Trojans, hardware, and backdoors) are difficult to detect [2].

The current authentication method is under a **centralized** authority agency, has several drawbacks, including being easily damaged, fraudulent and difficult to guarantee data security and transactions on educational institution services. From a technical point of view, educational services require reliable and operational authentication. According to a technical point of view, the technology that is suitable for educational digital authentication problems is a technology that uses distributed storage consensus technology for data storage and uses a decentralized infrastructure namely ledger technology or blockchain technology [3] [40]. Blockchain is considered a technology that has the potential to impact society while its potential remains largely unexplored [4]. Currently, blockchain can be divided into three forms depending on the application scenario, firstly private blockchain, consortium blockchain, and lastly public blockchain. Among the three types, with a consortium, blockchain members can

join and leave the blockchain network through an authority that has higher trust than public blockchains.

The blockchain that is often used by several institutions is the consortium blockchain. The consortium blockchain of the blockchain federation is a type of blockchain network where many organizations will perform maintenance on the system [5], and it is also semi-public and multi-centralized. With consortium blockchain, only consortium members can read and write data which can be used to protect personal data and ensure that data is not tampered with and also using consortium blockchain can streamline the authentication process and allow for increased speed in conducting transactions, to build trust without intermediaries , all transactions are bundled and stored locally in verified blocks on multiple devices belonging to different participants (nodes) of the network [6].

To overcome the problem of authentication in digital education, this paper will design **and implement authentication based on blockchain technology** as a solution. A total of 20% of the 2019 APBN and state revenues were allocated to the education sector with a value of Rp. 492.5 trillion, an increase of Rp. 4.6 t from the 2019 State Budget, with 123 PTN and 4547 PTS which in total there are 4670 Universities in Indonesia [47], so that the education sector is very interesting to implement using blockchain technology [7]. With blockchain, it allows effectiveness in ensuring information security, avoiding damage, data theft, and protecting the owner's access rights. In the system design in this paper, the authentication of the blockchain system uses digital certificates and is managed by a public key infrastructure, this solution ensures strong authentication and secure data on digital education [8]. The system to be created has several stages; first, smart contract design, then function of each module and lastly system testing which can later effectively realize the digital resource upload and authentication process.

2. Related Work

Bitcoin Appeared on January 3, 2009, created by someone under the pseudonym Satoshi Nakamoto, in 2008 Satoshi Nakamoto published a paper entitled "The Cryptography" mailing list on metzdowd.com describing the digital currency bitcoin using technology blockchains [9]. Blockchain is a block of data that is interconnected so that it looks like a chain, in short it will connect users without going through any intermediaries. So, each user will store each of the other user's data blocks [10]. This innovative technology is used in several applications such as education, business industry, healthcare, and governance because all transactions implemented on the blockchain are transparent, immutable and secure [34] [11]. From here, blockchain technology began to attract the attention of many people and became a global conversation [35]. According to a statistical survey, conducted in September 2015 by Statista, from 2014 onwards there has been a huge increase in blockchain technology funding investments worldwide. Blockchain technology uses multiple distributed nodes to generate and update data, uses cryptography to secure data transmission and access, and uses smart contracts to restrict and manipulate data. Based on this, blockchain technology can realize distributed data storage which will help humans in many ways.

The use of blockchain technology in smart contracts is the design chosen to address digital authentication of education, with the application of blockchain technology, the system no longer needs supervisors from regulatory agencies or third parties and ownership information of digital education resources can be stored on a distributed network of multiple nodes. Smart contracts are self-executed contracts (usually stored on the blockchain) whose terms are directly written into lines of code, although some parts still require human control [12]. Recently, the relationship of blockchain to smart contracts has received increasing attention from the media [42], and has begun to be referred to as "The Next Big Thing" [13], "The New Black", "The philosopher's stone" [14] or "The new Graal" [15]. The application of blockchain technology in educational service systems is based on the fact that blockchain technology has a relatively high fault tolerance supported by distributed nodes, and each node that participates in the system has a complete ledger copy [37]. Although there are some service anomalies in some nodes, the whole system can still guarantee normal operation, which allows the system to provide reliable technical support as well as central database

redundancy. Therefore, blockchain technology is believed to be able to effectively reduce fraud by ensuring every data in the system is transparent and managed in a decentralized manner [42].

In this paper, the system uses fabric as a technical solution to realize a suitable business model, because fabric has the characteristics of a fast transaction rate and scalability to meet business needs. The choice of fabric as a technical solution was inspired by the blockchain project on Hyperledger i.e. Hyperledger Fabric is an implementation of a distributed ledger platform for running smart contracts, leveraging known and proven technologies, with a modular architecture that allows implementation of various plugin-able functions [16] . Fabric will provide the grpc API and SDK for applications and applications can access the public ledger in the consortium blockchain by interacting APIs and SDKs [17] that use smart contracts and package the business logic and release it to the fabric network node.

3. Blockchain-based Education Digital Authentication System Blockchain

3.1 Authentication System Structure

In this paper, the system will use blockchain technology as a solution to digital education problems. The choice of this solution is based on the Hyperledger Fabric framework from the IBM consortium blockchain which will be used to design an authentication system that is tailored to the digital needs of education. The authentication process itself is a user validation process when entering the system and allows the user to access all services provided by the system without the need to enter the password repeatedly [18]. [19], authentication also allows us to ascertain who we are dealing with, giving trust to others so that we can control and manage potential risks in an action [20]. Authentication that is designed based on blockchain technology, in contrast to traditional authentication which has limitations and heterogeneity of resource devices, the existing security solutions are not fully adapted to the needs of the ecosystem [21], whereas in systems built using a blockchain network it has advantages; secure storage is hassle free, decentralized, and provides a decentralized and transparent transaction security solution between all parties involved.

The fabric network layer used as a technical solution in the system, will later be used to store data in educational digital, receive transaction verification, provide ownership queries and generate data blocks. In addition, the blockchain-based authentication system will be divided into three layers, the upper, middle and lower layers. First, the top layer or the main screen of the application which consists of the functions of registration, login, authentication of data ownership information, uploading data on digital education. Second, the middle layer or smart contract layer is a function that will be used to realize business processing logic. Third, the lower layer, namely the fabric network layer, in this layer, the node network has the same rights and obligations through the P2P protocol, which is a new technology that uses computing power and network bandwidth rather than depending on servers. The lower layers also use a consensus mechanism that is used to achieve consistency.
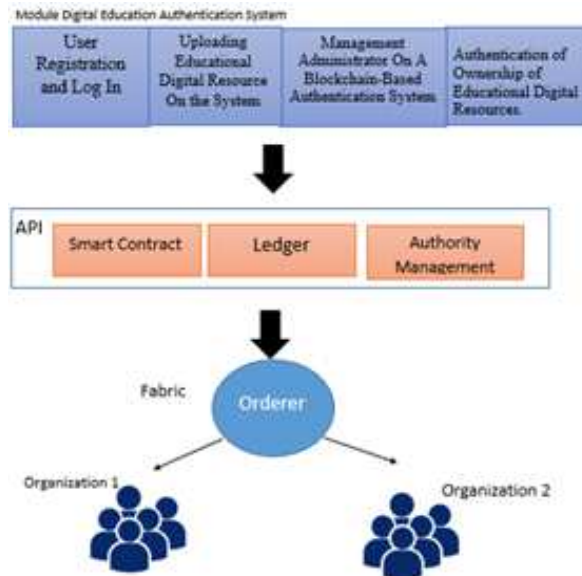
Figure 1. Educational Digital Authentication System Structure

3.2 Smart Contract Development on the Blockchain Authentication System Network

The education digital authentication system designed will introduce three aspects with **smart contracts** [23] consisting of, transactions, participants, and assets. Educational digital transaction objects refer to non-paper electronic media data such as optical and magnetic media, digital educational transaction objects can be categorized into two types, namely physical transaction objects (often in the form of text, images, sound, video, etc...) and service transaction objects. (such as one-to-one counseling services) [22]. For participants, it is divided into 2 parts, first as administrators to carry out transactions and users who have assets, who can download, use data, and upload resources on digital education. The participant's setting as a user consists of = {ID, which is a unique user identifier, password or password to login, name for user name, resource list Id of user owner, and finally email as the address used by the user to login}. Second, assets consist of tangible and intangible assets, assets in this case refer to data contained in digital education. for data, there are several elements, namely the name of the data, the RId or data id, the time of creation, and the type of format that contains the id of the asset owner. As for the transaction aspect, it refers to the interactions that occur in smart contracts.

In the education digital authentication system designed, there is a contract function consisting of several elements;

1. **Register Admin** is to register an administrator account.

2. **User Register is used** to register a user account.

3. **Check is** used to check user information.

4. **Query** means asking for educational resource information.

5. **Check Right** is to see the owner of educational resources.

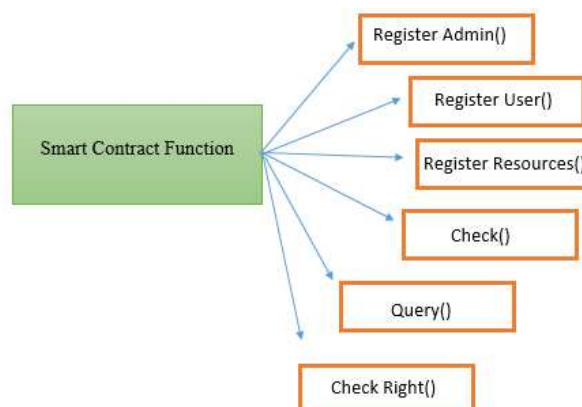6. **Register Resource** means uploading educational resources.

Figure2. Functions of Smart Contracts

3.3 Design of functions in a Blockchain-Based Authentication System

A blockchain technology-based authentication system for digital education designed, including:

1. Utilization of smart contracts used to transmit information and check delivery information.
2. Delivery of user identity information by utilizing smart contracts.
3. Utilization of smart contracts to achieve authentication of ownership on resources contained in digital education.
4. In the system design of this paper, there is timeliness in reading data, namely when resource information sent to a blockchain-based authentication system can be recorded directly in a local database

Figure 3. Education Digital Authentication Data Storage

3.3.1 User Registration and Login

The login function for the designed authentication system will use smart contracts for verification to match the authenticity of data [24] and also for registration of new users, which later with the smart contract will receive requests then sent to the administrator, if it fails then you have to start over from the beginning. Account registration, including data on first name, last name, email and password then select the sign up button to complete the registration process [25], and the login function will be successful if the comparison of the entered identity is the same as the data that has been stored.
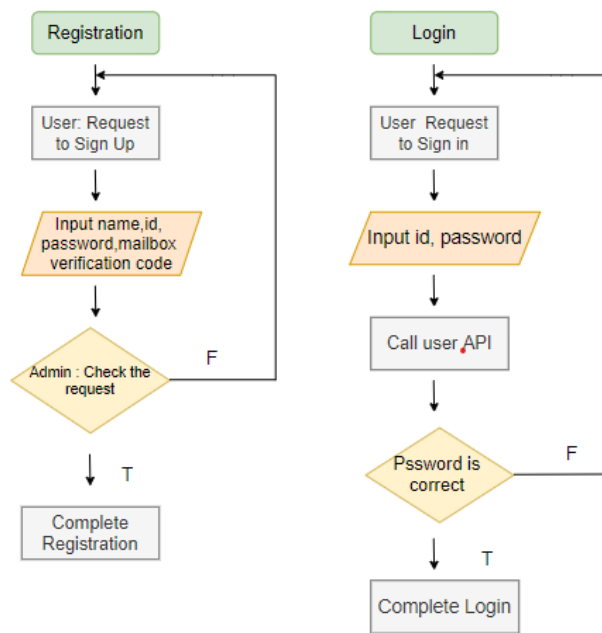
Figure 4. Registration and Login Process

3.3.2 Function of uploading educational digital resources

In the system to be designed, it is possible to upload user original resources into educational digital resources which are used for business needs. Resources that have been successfully verified will be stored permanently on the blockchain platform [45] to ensure data authenticity and avoid data corruption or data theft [39].
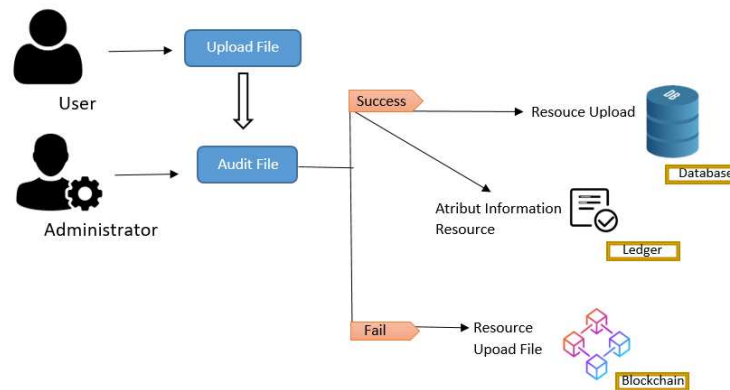

Figure 5. File Upload Process

3.3.3 Function of downloading digital resources

In using the download function in the designed system, it will pass several verification stages to be able to download or use data that has been stored on the blockchain network. The first stage, based on the data that has been stored into the blockchain network, will ask some relevant things according to the data on the blockchain. The second stage, with a smart contract, the system will automatically match the information. Based on these stages, digital education authentication is complete because only users who get permission can use data in digital education, and those who do not have access or fail in the verification stage will not be able to use the data arbitrarily.
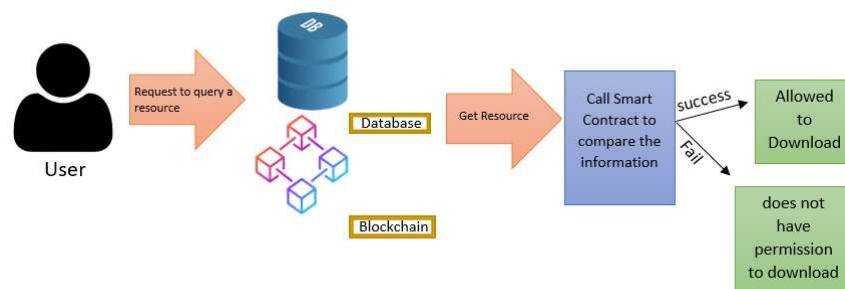
Figure 6. Function of Downloading Digital Authentication Data

3.3.4 Administrator on blockchain-based authentication system

The administrator's task in the way the authentication system is designed, the administrator will be able to see all information ranging from user information, operation and even review the running status contained in the blockchain system . For certification of ownership and upload of educational digital resources will be supervised by administrators in terms of ensuring ownership certification and verification of legality of uploaded resources before being stored in the blockchain and database [42]. For illegal resources allowed to be stored by the user or directly backed up into the library file failed to pass the audit.

4.Selection of Fabric Network on Blockchain Based Education Digital Authentication

In the design of the authentication system, the network fabric will be applied to the Ubuntu system which is used in building and developing the business model as well as the utilization of the composer reset server which is used to generate the business model API. With the implementation of blockchain-based authentication, nothing will be able to tamper with transaction records because every time a user uploads transaction log information, it will be immediately packaged into a block by another node and only through access can the function be executed.

4.1 Application of Hyperledger Composer in system platform development Platform

Development on a blockchain based authentication system **will use** a blockchain **network supported by fabric** and utilize hyperledger composer in business program development and completion of interactions between web pages and blockchain. The stages that are passed in the development of an educational digital authentication platform:

1. First, on the ubuntu 16.04 system, a business network will be created by the system.

2. Then, the business network will be used to develop smart contracts through modeling languages and APIs. The business network will also interact with hyperledger composers.

3. Third, through the rest server composer, the system that has been designed will interact with the blockchain network.

4.2 Smart contracts as system business logic

In the rapid development of web interaction interfaces, digital authentication systems utilize composers and smart contracts in building collaborative tools of blockchain commercial networks. In a digital system based on blockchain technology, the writing of the relevant files will use the help of smart contracts. The categories of files contained in the system include;

1. The qry file used to provide the query interface.

2. Acl file, which will be used for granting permissions.

3. js file, to explain the business logic.

4. CTO file, which will be used in determining the business network model on asset participants, and transactions.

In a system, there is a requirement that must be met as well as the educational digital authentication system designed in this paper, meeting the requirements of a system. In this system design, assets are used as resources, model files define admins and users as participants, and finally for transactions determined by writing business logic, there are check rights, check queries, resource registers, and user registers. And lastly, in the establishment of a remote interface business model achieve smart contracts, using the rest server composer.
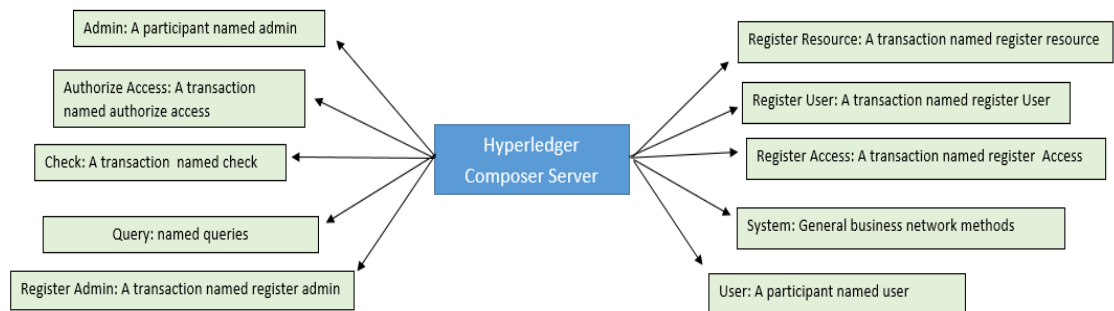

Figure 7. Composer Server

4.3 Functions of a blockchain-based authentication system

4.3.1 Registration and participant account login functions

The stages that users will go through in registering an account for the design of an educational digital authentication system in this paper:

1. the user will input the relevant data into the system .

2. Users will be prompted for a password twice to strengthen account security.

3. The Register User API will perform its duties in generating user information such as, password, name, id, mailbox, if the data entered into the system has been verified correctly, user information will be used to mark the id, and the transaction as a status to be confirmed.

4. Furthermore, the data that has been inputted will be reviewed by the administrator with verification of completion of account registration which will be forwarded to the blockchain network.

How the system works in confirming user login: The

1. user will input the id and password that have been created.

2. Then, to confirm the data entered by the user is the same as the data stored on the blockchain network, the system will call the API to do its job.

3. After confirmation that the inputted data is the same as the stored data, the user login has been successfully carried out.

Figure 8. User Login and Registration Display

4.3.2 Function of uploading educational digital resources on the system

The stages that users go through to upload files into the system: The

1. users will be asked to fill in information about the resource file to be uploaded.

2. The user will select a file and start uploading the selected resource file.

3. Next, for generating information about the resource description uploaded into the transaction, the system will call the API to generate information about the name, id, creation time, id of the resource owner.

4. The administrator will verify the uploaded resources.

5. The verified resource files will be directly stored in the blockchain network database.

Figure 9. Information Display of Education Digital Data

4.3.3 authentication of digital education resource ownership.

In the design of the ownership system of uploaded educational digital resources, the owner can know, so that people who do not have access will not be able to use them [33]. The

following are the stages of the system in verifying the owner of educational digital resources.

1. The system will ask relevant questions regarding the owner id and owner information of digital resources stored in the database and blockchain, when there are users who want to download.

2. To verify, the system will call the API check right, if verification fails the user is not the owner of the digital resource and is unable to consult or download the desired digital resource.
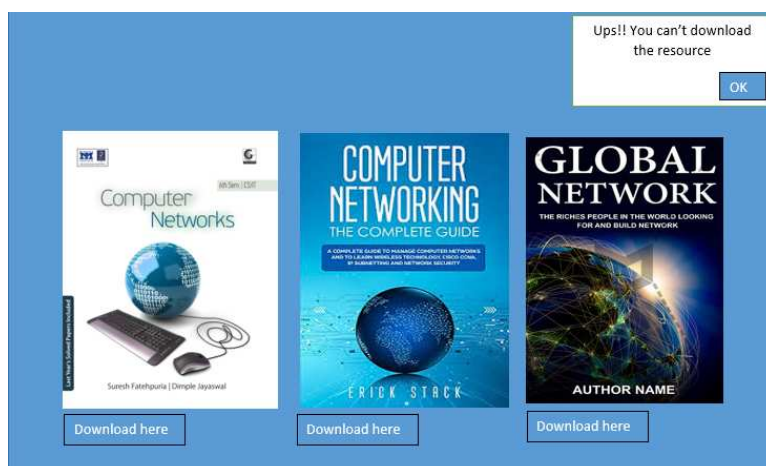

Figure 10. Education Digital Data Ownership Information

4.3.4 management administrator on blockchain-based authentication system

Administrator duties on the designed education digital authentication system:

1. After the resource file is uploaded by the user, the administrator will use the query API to query the list of unaudited resources .

2. Next, with the API the system will verify the validity of the user uploaded resources.

3. For successfully verified resources will be directly stored in the blockchain network database.

4. Resources that fail to be verified will be denied requests by audit.

Figure 11. Data Information Audit

5. Conclusion

Industrial revolution 4.0 is generally known as a change in the way of work that focuses on data management, industrial work systems through technological advances, communication and work efficiency improvements related to human interaction [38]. In this paper, we will review the application of blockchain technology that does not concentrate on the cryptocurrency field. This paper refers to the application of blockchain in education which refers to socio-technological indicators [26]. After analyzing the problems that exist in traditional authentication in the education sector that still uses verification management methods by a centralized authority, the system designed in this paper will combine digital authentication with blockchain consortium technology which is popularly used by several institutions as a solution to traditional authentication problems. Authentication of large-scale Internet devices safely and reliably is not trivial with today's network frameworks and existing security mechanisms [27]. To overcome these authentication problems blockchain offers an elegant solution. Therefore, in this paper we will use blockchain for authentication systems that are applied to digital education. This is based on the fact that in the world of technology, the existence of blockchain is a very dramatic improvement to collect information, distribute and manage information. Blockchain is also a decentralized distributed database. and without permission [28]. The combination of knowledge between the fields of education and blockchain technology will create a new revolution of the education industry which is deemed stagnant and not in accordance with the current developments [29]. However, as with cryptographically secured technology blockchain can be used for good and evil regardless of the benefits [30].

In the system design, the blockchain will provide a decentralized method for digital education resources, authenticate resource ownership information with private key, guarantee that there will be no damage to digital resources, and protect the rights and interests of digital resource owners. The system mode solution that has been designed can be applied to a learning management system where students can download resources stored on the system, and teachers can upload resource files into digital education. By implementing an authentication system based on blockchain technology, it will protect proprietary information without interference or data theft.

6. Acknowledgement

References

[1] S. D. K. Hu et al., "Implementasi Blockchain: Studi Kasus e-Voting," IJRTI, vol. 16, no. 1, pp. 183–189, 2018.

[2] S. Panja and B. K. Roy, "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain.," IACR Cryptol. ePrint Arch., vol. 2018, p. 466, 2018.

[3] P. Baudier, G. Kondrateva, C. Ammi, and E. Seulliet, "Peace engineering: The contribution of blockchain systems to the e-voting process," Technol. Forecast. Soc. Change, vol. 162, p. 120397, 2021.

[4] S. K. Vivek, R. S. Yashank, Y. Prashanth, N. Yashas, and M. Namratha, "E-voting systems using blockchain: An exploratory literature survey," in 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), 2020, pp. 890–895

[5] I. Handayani, E. Febriyanto, and A. Jethro, "Designing Popular Classes on Viewboard Public Assessment of Lectures Based on YII Framework," Aptisi Trans. Technopreneursh., vol. 1, no. 2, pp. 144–156, 2019.

[6] I. U. Rahardja and S. Raharja, "Artificial informatics," 2009 4th IEEE Conf. Ind. Electron. Appl. ICIEA 2009, pp. 3064–3067, 2009, doi: 10.1109/ICIEA.2009.5138764.

[7] T. E. H. Setia and A. Susanto, "Smart Contract Blockchain pada E-Voting," J. Inform.

Upgris, vol. 5, no. 2, 2019.

[8] U. Rahardja and E. P. Harahap, "Implementation of Information Planning and Strategies Industrial Technology 4.0 to Improve Business Intelligence Performance on Official Site APTISI," in Journal of Physics: Conference Series, 2019, vol. 1179, no. 1, p. 12111..

[9] M. Hardini, Q. Aini, U. Rahardja, R. D. Izzaty, and A. Faturahman, "Ontology of Education Using Blockchain: Time Based Protocol," 2020, doi: 10.1109/ICORIS50180.2020.9320807.

[10] U. Rahardja, Q. Aini, M. D. A. Ngadi, M. Hardini, and F. P. Oganda, "The Blockchain Manifesto," 2020, doi: 10.1109/ICORIS50180.2020.9320798.

[11] U. Rahardja, N. Lutfiani, A. S. Rafika, and E. P. Harahap, "Determinants of Lecturer Performance to Enhance Accreditation in Higher Education," in 2020 8th International Conference on Cyber and IT Service Management (CITSM), 2020, pp. 1–7, doi: 10.1109/CITSM50537.2020.9268871.

[12] S. Dubai, "Dubai blockchain strategy," Smart Dubai, Dubai Gov. Dec, 2016.

[13] Sudaryono, U. Rahardja, Q. Aini, Y. Isma Graha, and N. Lutfiani, "Validity of Test Instruments," J. Phys. Conf. Ser., vol. 1364, no. 1, 2019, doi: 10.1088/1742-6596/1364/1/012050.

[14] F. P. Oganda, N. Lutfiani, Q. Aini, U. Rahardja, and A. Faturahman, "Blockchain Education Smart Courses of Massive Online Open Course Using Business Model Canvas," in 2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS), 2020, pp. 1–6.

[15] N. Shanthi, R. Suvitha, and R. C. Suganthe, "Blockchain based e-voting approach IN P2P network," J. Crit. Rev., vol. 7, no. 9, pp. 337–342, 2020.

[16] A. Alam, S. M. Z. U. Rashid, M. A. Salam, and A. Islam, "Towards blockchain-based e-voting system," in 2018 International Conference on Innovations in Science, Engineering and Technology (ICISET), 2018, pp. 351–354.

[17] U. Rahardja, A. N. Hidayanto, N. Lutfiani, D. A. Febiani, and Q. Aini, "Immutability of Distributed Hash Model on Blockchain Node Storage," Sci. J. Informatics, vol. 8, no. 1, pp. 137–143, 2021.

[18] F. Agustin, Q. Aini, A. Khoirunisa, and E. A. Nabila, "Utilization of Blockchain Technology for Management E-Certificate Open Journal System," Aptisi Trans. Manag., vol. 4, no. 2, pp. 133–138, 2020.

[19] I. Handayani, D. Supriyanti, G. Maulani, and N. Lutfiani, "The ilearning journal center: Education startup to enhance lecturer research," Int. J. Adv. Trends Comput. Sci. Eng., vol. 9, no. 4, pp. 4678–4682, 2020, doi: 10.30534/ijatcse/2020/70942020.

[20] Q. A. Henderi, N. P. L. Santoso, A. Faturahman, and U. Rahardja, "A proposed gamification framework for smart attendance system using rule base," J. Adv. Res. Dyn. Control Syst, vol. 12, no. 2, pp. 1827–1838, 2020.

[21] Q. Aini, A. Badrianto, F. Budiarty, A. Khoirunisa, and U. Rahardja, "Alleviate fake diploma problem in education using block chain technology," J. Adv. Res. Dyn. Control Syst., vol. 12, no. 2, pp. 1821–1826, 2020.

[22] Q. Aini, U. Rahardja, N. P. L. Santoso, and A. Oktariyani, "Aplikasi Berbasis Blockchain dalam Dunia Pendidikan dengan Metode Systematics Review," CESS (Journal Comput. Eng. Syst. Sci., vol. 6, no. 1, pp. 58–66

[23] Q. Aini, U. Rahardja, M. R. Tangkaw, N. P. L. Santoso, and A. Khoirunisa, "Embedding a Blockchain Technology Pattern Into the QR Code for an Authentication Certificate," J. Online Inform., vol. 5, no. 2, 2020.

[24] U. Rahardja, A. N. Hidayanto, T. Hariguna, and Q. Aini, "Design framework on tertiary education system in Indonesia using blockchain technology," in 2019 7th International Conference on Cyber and IT Service Management (CITSM), 2019, vol. 7, pp. 1–4.

[25] H. L. J. U. R. K. Chandra Lukita Ninda Lutfiani, "Miu Ai: Application Based on The ECommerce Prototype for Japanese Otaku in Indonesia," J. Adv. Res. Dyn. Control Syst., vol. Volume 12, no. Issue 6, pp. 618–623, 2020, doi: 10.5373/JARDCS/V12I6/S20201071.

[26] Q. Aini, T. Hariguna, P. O. H. Putra, and U. Rahardja, "Understanding how gamification influences behaviour in education," Int. J. Adv. Trends Comput. Sci. Eng., vol. 8, no. 1.5, pp. 269–274, 2019.

[27] A. Dudhat, N. P. L. Santoso, S. Santoso, and R. Setiawati, "Blockchain in Indonesia University: A Design Viewboard of Digital Technology Education," Aptisi Trans. Technopreneursh., vol. 3, no. 1, pp. 68–80, 2021.

[28] M. Prawira, H. T. Sukmana, V. Amrizal, and U. Rahardja, "A Prototype of Android-Based Emergency Management Application," 2019 7th Int. Conf. Cyber IT Serv. Manag. CITSM 2019, 2019, doi: 10.1109/CITSM47753.2019.8965337.

[29] K. Curran, "E-Voting on the Blockchain," J. Br. Blockchain Assoc., vol. 1, no. 2, p. 4451, 2018.

[30] Q. Aini, N. Lutfiani, N. P. L. Santoso, S. Sulistiawati, and E. Astriyani, "Blockchain For Education Purpose: Essential Topology," Aptisi Trans. Manag., vol. 5, no. 2, pp. 112–120, 2021.