Blockchain Encryption on Student Academic Transcripts using a Smart Contract

Primasatria Edastama[1], Ninda Lutfiani[2], Qurotul Aini[3], Suryari Purnama[4], Isabella Yaumil Annisa[5]

[1] Economics and Business, Esa Unggul University, Indonesia
Email: primasatria@esaunggul.ac.id
[2] Information Technology, University of Raharja, Indonesia
Email: ninda@raharja.info
[3] Engineering, Universiti Teknologi Malaysia, Malaysia
Email: qurotul@graduate.utm.my
[4] Economics and Business, Esa Unggul University, Indonesia
Email: suryari.purnama@esaunggul.ac.id
[5] Information Technology, University of Raharja, Indonesia
Email: Isabella@raharja.info

Abstract. As an innovation in the world of computers, blockchain has many benefits and is also widely applied in the world of education. Blockchain itself has many advantages, especially in the world of education. Blockchain is a digital data storage system that consists of many servers (multiserver). In this Blockchain technology, data created by one server can be replicated and verified by another server. By using this technology with a decentralized system and strong cryptography and can help colleges or universities to build infrastructure in the archive storage of transcripts, diplomas, and diplomas. Usage One of the blockchain technology applications in education is iBC, namely the e-learning Blockchain Certificate, book copyright, and also e-Portfolios. iBC or e-learning Blockchain Certificate is a tool designed to create, verify and also issue blockchain certificates. As has been supported by the IBC to create certificates that are globally verified and stored in a decentralized manner. Here will be presented use cases that are relevant in the use of Blockchain technology in educational environments, especially data processing in universities and we also try to design an IBC based on blockchain technology that can be used to support transparency and accountability of colleges or universities in issuing diplomas and grades.

Keywords: : Blockchain; Transcript; iBC; Process Data; Digital

INTRODUCTION:

Blockchain is an information technology that has been widely applied in daily needs. This technology is realized using the concept of decentralization and data processing(Yusup et al., 2019). Blockchain data stored in data records will permanently be communicated peer-to-peer in the information technology network.

Blockchain is also considered to use a digital data storage system consisting of multiple servers (multiserver). In this Blockchain technology, data that is formed by one server can be replicated and verified by another server (Heryanto, 2020). The use of Blockchain is not limited to cryptocurrencies.

In the case of education, there are many fake diplomas. This fake diploma is often used to become a government official, become an employee, and even other things that could be considered a crime. Because this occurs when it is difficult to verify diplomas or student academic transcripts (Winarno, 2019).

(Firliana et al., 2020). The technology that applies this is iBC. iBC is built with blockchain which provides accountability and transparency in the storage of diplomas and certificates. In other cases, the use of this technology is equipped with strong cryptography and guaranteed integrity of records and valid certificates and certificates. Based on this, an e-transcript design was created using blockchain technology (Sriwiji, 2019).

Blokchain. In blockchain technology, there are key characteristics, such as persistence, anonymity, decentralization, and auditing capabilities. Blockchain technology is able to work in a decentralized environment, only by enabling and integrating some of the core technologies such as cryptographic hashes, digital signatures (based on asymmetric cryptography) and distributed consensus mechanisms (Zheng et al., 2018). So that transactions on blockchain technology can be carried out in a decentralized manner.

Blockchain is a floor-breaking era that allows new styles of allotted software program architectures, wherein components can discover agreements on their shared states for decentralized and transactional facts sharing via a wide community of untrusted users, without

In the above problem, a system for reporting assessments that can be accessed globally and has good availability is needed counting on a relevant factor of integration that must be depended on via way of means of anything within the framework (Sunarya & Lutfiani, 2020). The facts shape blockchain as a time-stamped block list, which tracks and aggregates facts about transactions that have ever befallen in the blockchain community. Thus, the blockchain offers an unchangeable garage of facts that most effectively permits transactions to be inserted without updating or deleting any current transaction on the blockchain to save you tampering and revision (Rahardja, Lutfiani, et al., 2019). Blockchain's maximum well-known utility is cryptocurrencies, which during the final 12 months become a massive phenomenon because of their promising use of the era.Blockchain is also a rule in a science computer that has the purpose of knowing data sharing and its structure (Sudaryono et al., 2019). However, Blockchain is now the "fifth evolution" of current computing development so that the blockchain is defined as a data structure that allows us to create digital books from data and share data in the network. Every block in the Blockchain will always be associated with the previous block and the block that follows it.
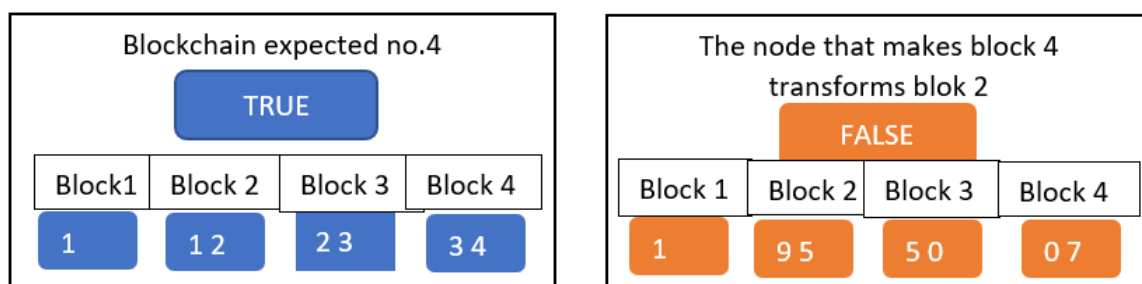

Figure1. Shows how blockchain technology can overcome blockchain hacking

The types of blockchains that exist today:
1. Permissive Blockchain

Permissive Blockchain, namely Blockchain that puts conditions for development in making systems on the Blokcain network. Available origin code is open or not.
2. Public Blockchain

The Public Blockchain is the Blockchain that is widely distributed and works using native tokens. The blockchain is open source so that everyone can participate (contribute) in maintaining the blockchain.
3. Private Blockchain

The Private Blockchain is a Blockchain that has a small scale of use and does not require a local token.It is a favorite for consortium participants who have trusted members.

All of the Blockchain above uses cryptographic functions to allow participants (nodes) in a particular network to manage the ledger securely without involving a third party as control.

The advantages of Blockchain that can be used in carrying out system design: (1) Accuracy; (2) Anonmymity; (3) Autonomy; (4) Fairness; (5) Forgiveness; (6) Transparency; (7) Security

iBC stands for ilearning Blockchain Certificate. The ilearning Blockchain Certificate (iBC) is an open standard used to issue and verify official documents designed using blockchain technology. Digital records that are registered in blockchain technology will be cryptographically signed, shareable, and temper-proof. The purpose of creating the ilearning Blockchain Certificate (iBC) is to invite every individual to always innovate about owning and sharing their official documents.

iBC is an open standard used to verify and publish official documents that have been designed with Blockchain technology. Digital records registered in Blockchain, cryptographically signed, shareable and temper-proof (Aini, Rahardja, et al., 2020). The purpose of creating iBC is to invite everyone to innovate in sharing (Alwiyah & Sayyida, 2020).

METHOD

This study uses the SLR (Systematic Literature Review) method where this method is a method that identifies, assesses, and interprets meetings on a research topic to answer predetermined research questions (Suhartono, 2017). In this research data collection the technique used is to collect many national and international journals and evaluate and interpret and some of these research journals.

Our research objective is to show that many cases have been resolved using Blockchain technology. For approximately ten years since the technology was first introduced, blockchain users have grown in various regions. This relevant experience provides us with the opportunity to discuss some of the issues that have arisen over the last few years.

In this journal, a systematic literature review approach is followed according to the guidelines proposed by Kitchenham (Kitchenham et al., 2009). To cover a broad spectrum as well as relevant publications, we decided to look for electronic libraries that use ACM Digital Library, IEEE Xplore Digital Library, Science Direct, Blockchain for Applications 200, and Springer link. The keyword strings we use are: "BLOCKCHAIN AND E-CERTIFICATE", "BLOCKCHAIN AND EDUCATION". In the next step, we searched for keyword strings in the paper title, abstract, and keywords. We also limit our search and also select content types to only journals and conference papers, as well as reject unsuitable book chapters or web pages. The procedure for selecting literature will be carried out in November 2021, so that it contains published or indexed papers up to that date. The number of final papers we submitted after deleting duplicates was 200. Then, manually we excluded papers whose titles seemed irrelevant to our research. We reduced the papers to 100 to 40 papers. We read the entire text of this paper, culminating in 26 of them to extract information and answer our research questions.
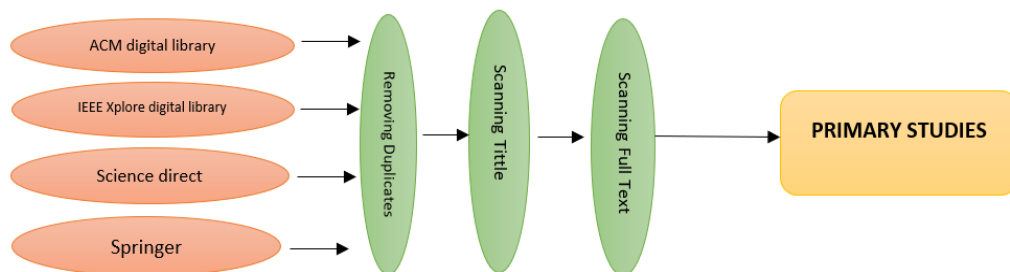

Figure 2. Procedure for identifying primary studies

RESULTS AND DISCUSSION

Result

The design of the e-transcript scheme in Blockchain technology uses two stages (Riza, 2020). The first is the publication of transcripts and the second is the issuance of certificates. (a)

The grade transcripts are issued by the University based on the scores obtained by each student in the semester; (b) Students are the parties entitled to receive the transcript so that the transcript is added to the public key (blockchain address); (c) After that the transcript is processed so that it can be entered into the blockchain; (d) Students take transcripts and save transcripts in the client application.
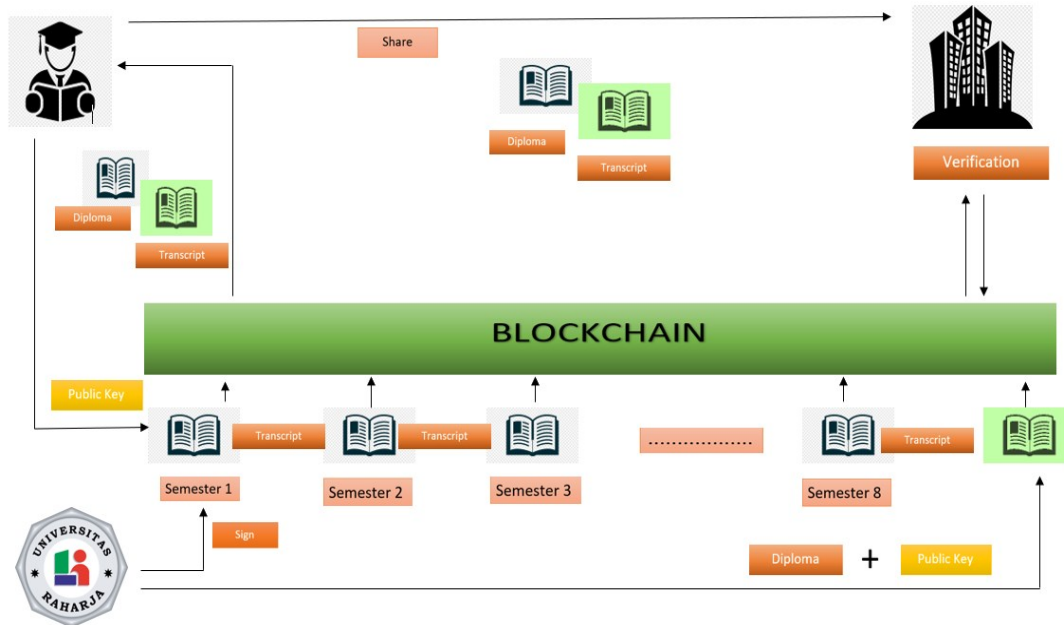

Figure 2. The application Technology

The application of blockchain technology can be used to reduce the occurrence of fake diplomas. With this, the University (agency) can issue diplomas through applications that are already available.

Advantages of e-Transcripts. The advantages of blockchain e-transcripts:

1. Resistant to DDOS Attack

The application of e-Transcript with Blockchain technology can prevent the server from going down against DDOS Attack. DDOS Attack on e-transcripts applied to the bitcoin network will drain a lot of system resources or money. Because each attacker floods the transaction and will be charged a fee. This attempt is done to the point of paralyzing the system and will be very costly (Mirkovic & Reiher, 2004).

2. Data Integrity

The application of e-Transcript in Blockchain technology can protect the stored data from people who want to change the data without their knowledge (Yusup et al., 2018). The process of changing data on the blockchain system will make the attacker perform a challenge system at each block formation so that the block forms a chain that is longer than the original chain (Safrizal & Budiadyana, 2019).

3. Transparency

The diploma and transcript data will be recorded by the blockchain. To carry out audit activities, complete data will be available which can be used by every agency or every person (Aini, Badrianto, et al., 2020).

4. Security

The resulting diploma and transcript can be used by students who already have a public key that is entered in the blockchain. Each diploma and transcript will only correspond to one private key that is owned by the certificate holder and the value transcript.

5. Autonomy

Records of all data will be distributed in a decentralized manner so that the node has transcripts and diplomas (Fajar, 2020). Such (decentralized) storage will lower the risk of server downtime and data loss(Riza et al., 2019).

6. Anonymity

The e-transcript uses public keys to generate private and public keys for students. The private key will be stored in the student client application and will be published publicly so that it can be used for the verification process and sending documents from students to the

desired place, for example, a job-seeking agency or university (Aini et al., 2019).

Discussion

According to research findings, this new technology applies the concept of blockchain to education
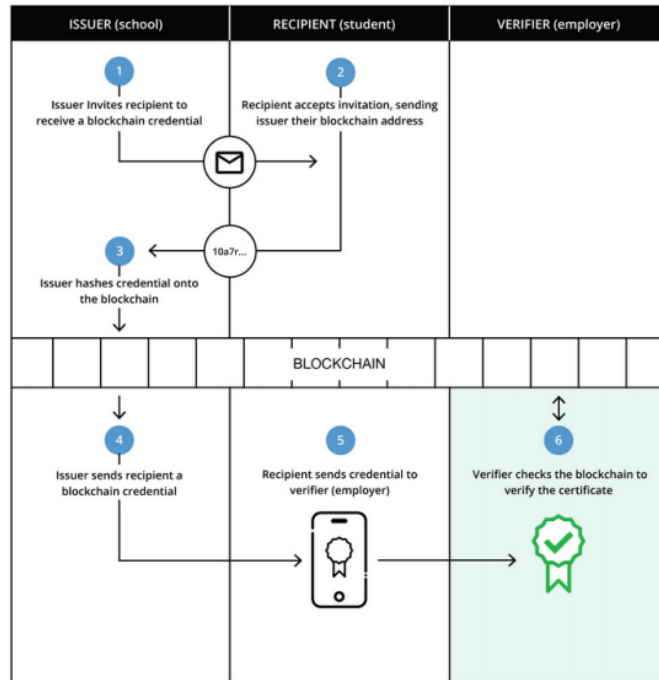

Figure 3. The work Process

One of the stages of a certificate falsification problem is achieved any updates being made. Certification is the process of granting certificates that have met certain requirements, namely having qualifications academic, competent, physically and mentally healthy, and has the ability to realizing the goals of national education, which is accompanied by an increase in decent welfare (Muslich, 2007: 12). Raharja University is of course so focused for the services provided to students as Raharja, the only one is a certificate whose data is very accurate. Before that could happen, there was a certificate flow process that ran before the technology was used blockchain. Starting from the university or college or publisher inviting students or students to receive blockchain credentials, then the student or recipient sends the blockchain address to the university or college (publisher), after which the university or college characterizes the credentials on the blockchain, then the publisher sends blockchain credentials, after which the student sends a verification to the verifier, and the final verification process will check the blockchain to verify the certificate.

Scoring system

The system of taking academic scores in tertiary institutions can be seen in the Regulation of the Minister of Cultural Education No. 3 of 2020, namely the National Standards for Higher Education in the fifth part of article 21 and the principles in article 22. Sounds from articles 21 and 22 Permendikbud No.3 2020, namely:

A. Learning assessment standards are the minimum criteria for process assessment and student learning outcomes to fulfill graduate learning outcomes.

B. Assessment of student learning processes and outcomes as referred to in paragraph (1) includes:

C. Principles of Assessment: (1) Assessment instrument technique; (2) Assessment mechanisms and procedures; (3) Implementation of the assessment; (4) Reporting assessment; (5) Graduation.

It can be seen that the assessment process requires principles that include authentic, educational, accountable, objective, and transparent (article 19 paragraph 1). As well as this explanation, we can see in chapter 19 verse 2 to verse 6: (a) The educational principle is that assessment is to motivate students to be able improve planning and learning methods, and be able to achieve results learning; (b) The authentic principle is an assessment that is

oriented towards a learning process continuous and learning outcomes reflect the ability of students at during the learning process; (c) The principle of accountability is an assessment carried out by procedures and clear criteria agreed upon at the beginning of the lecture and understood by students; (d) The principle of transparency is an assessment that the procedures and results of the value can be accessible to all stakeholders.

The method used is a literature study of cases such as certificate falsification, iBC implementation, blockchain, and Regulation of the Minister of Education and Culture No.3 of 2020 concerning Higher Education National Standards (Rahardja, Harahap, et al., 2019). The design was made based on the iBC system by adjusting the higher education regulations in Indonesia (Permendikbud No.3 of 2020).

The projected platform takes the advantage of the blockchain in order to form a globally trusty higher education credit and grading system (Fauziah et al., 2021)(Hardini et al., 2020). As a signal of concept, we tend to conferred a prototype implementation of the system platform that is predicated on the ASCII text file Ark blockchain platform. The proposed system platform addresses a globally unified viewpoint for college kids and organizations. Students profit from one and clear read of their completed courses, whereas have access to up thus far knowledge notwithstanding a student's academic origins (Agustin et al., 2020). alternative beneficiaries of the proposed system are potential employers, who will directly validate the knowledge provided by students. The projected solution is predicated on the distributed P2P network system. It transfers the upper education grading system from the current real-world physical records or ancient digital ones (e.g. databases) to AN efficient, simplified, present version, based on blockchain technology (Rahardja, 2009). it's anticipated that such a system may probably evolve into a unified, simplified and globally present education credit and grading system.

CONCLUSIONS AND SUGGESTIONS

The use of blockchain technology in education is no different from the application of blockchain technology in other fields. Many things in education can be applied with blockchain technology, one of which is this E-transcript.

Conclusions obtained from e-Transcripts using Blockchain technology: (1) The advantages of e-transcripts that are designed using blockchain technology are that they are resistant to DDOS attacks, maintain data integrity, transparency, security, autonomy, and anonymity; (2) E-Transcripts can be a solution to prevent counterfeiting of academic grades based on the advantages possessed by blockchain; (3) The e-Transcript design that uses blockchain technology has several stages, namely the stage of issuing transcripts, issuing certificates, and verification of documents.

REFERENCES

Agustin, F., Oganda, F. P., Lutfiani, N., & Harahap, E. P. (2020). Manajemen Pembelajaran Daring Menggunakan Education Smart Courses. *Technomedia Journal*, *5*(1), 40–53.

Aini, Q., Badrianto, A., Budiarty, F., Khoirunisa, A., & Rahardja, U. (2020). Alleviate Fake Diploma Problem In Education Using Block Chain Technology. *Journal of Advanced Research in Dynamical and Control Systems*, *12*(2), 1821–1826. https://doi.org/10.5373/JARDCS/V12I2/S20201225

Aini, Q., Rahardja, U., Handayani, I., Hardini, M., & Ali, A. (2019). Utilization of google spreadsheets as activity information media at the official site alphabet incubator. *Proceedings of the International Conference on Industrial Engineering and Operations Management*, *7*, 1330–1341.

Aini, Q., Rahardja, U., & Khoirunisa, A. (2020). Blockchain Technology into Gamification on Education. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*,

14(2), 1–10. https://doi.org/10.22146/ijccs.53221

Alwiyah, A., & Sayyida, S. (2020). Penerapan E-Learning untuk Meningkatkan Inovasi Creativepreneur Mahasiswa. *ADI Bisnis Digital Interdisiplin Jurnal*, *1*(1), 35–40.

Fajar, M. H. (2020). *Quality of service ethereum blockchain berbasis IPFS untuk validasi ijazah sekolah*. UIN Sunan Ampel Surabaya.

Fauziah, Z., Latifah, H., Rahardja, U., Lutfiani, N., & Mardiansyah, A. (2021). Designing Student Attendance Information Systems Web-Based. *Aptisi Transactions on Technopreneurship (ATT)*, *3*(1), 23–31.

Firliana, R., Indriati, R., Farida, I. N., & Niswatin, R. K. (2020). APLIKASI E-KATALOG YUDISIUM BUKTI PENGAMBILAN IJAZAH DAN TRANSKRIP NILAI. *Jurnal Inkofar*, *1*(2).

Hardini, M., Aini, Q., Rahardja, U., Izzaty, R. D., & Faturahman, A. (2020). Ontology of Education Using Blockchain: Time Based Protocol. *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, 1–5.

Heryanto, Y. (2020). *Purwarupa Sistem Verifikasi Sertifikat Pelatihan Kerja Berbasis Blockchain Pada Bbplk Bandung*. Universitas Komputer Indonesia.

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and Software Technology*, *51*(1), 7–15.

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39–53.

Rahardja, U. (2009). Artificial informatics. *2009 4th IEEE Conference on Industrial Electronics and Applications, ICIEA 2009*, 3064–3067. https://doi.org/10.1109/ICIEA.2009.51387 64

Rahardja, U., Harahap, E. P., & Dewi, S. R. (2019). The strategy of enhancing article citation and H-index on SINTA to improve tertiary reputation. *Telkomnika (Telecommunication Computing Electronics and Control)*, *17*(2), 683–692. https://doi.org/10.12928/TELKOMNIKA. V17I2.9761

Rahardja, U., Lutfiani, N., & Juniar, H. L. (2019). Scientific Publication Management Transformation In Disruption Era. *Aptisi Transactions On Management*, *3*(2), 109–118.

Riza, B. S. (2020). Blockchain Dalam Pendidikan: Lapisan Logis di Bawahnya. *ADI Bisnis Digital Interdisiplin Jurnal*, *1*(1), 41–47.

Riza, B. S., Mashor, M. Y., & Haryanto, E. V. (2019). THE APPLICATION OF RSA AND LSB IN SECURITY OF MESSAGES ON IMAGERY. *ADI Journal on Recent Innovation (AJRI)*, *1*(1), 20–32.

Safrizal, G. N. B., & Budiadyana, G. N. (2019). Analysis Application Design Career Development Center In The STMIK Insan Pembangunan and (Case Study: Information Study Program). *IAIC Transactions on Sustainable Digital Innovation*, *1*(1), 66–77.

Sriwiji, R. (2019). *Studi Empiris Pada Pemodelan Dan Prediksi Harga Bitcoin berdasarkan Informasi Blockchain Menggunakan Bayesian Regularization Neural Network*.

Sudaryono, Lutfiani, N., Suseno, & Aini, Q. (2019). Empirical Study of Research Performance Leading to Education 4.0 using the iLearning Method. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(1.5), 264–268. https://doi.org/10.30534/ijatcse/2019/4681. 52019

Suhartono, E. (2017). SYSTEMATIC LITERATUR REVIEW (SLR): METODE, MANFAAT, DAN TANTANGAN LEARNING ANALYTICS DENGAN METODE DATA MINING DI DUNIA PENDIDIKAN TINGGI. *INFOKAM*, *13*(1).

Sunarya, P. O. A., & Lutfiani, N. (2020). Analisis Sistem Sertifikasi Profesi Untuk Pengembangan Kompetensi Mahasiswa. *ADI Bisnis Digital Interdisiplin Jurnal*, *1*(1), 70–77.

Winarno, A. (2019). Desain E-Transkrip dengan

Teknologi Blockchain. *Prosiding Seminar Nasional Pakar*, 1–37.

Yusup, M., Aini, Q., Apriani, D., & Nursaputri, P. (2019). PEMANFAATAN TEKNOLOGI BLOCKCHAIN PADA PROGRAM SERTIFIKASI DOSEN. *SENSITIf: Seminar Nasional Sistem Informasi Dan Teknologi Informasi*, 365–371.

Yusup, M., Naufal, R. S., & Hardini, M. (2018). Management of Utilizing Data Analysis and Hypothesis Testing in Improving the Quality of Research Reports. *Aptisi Transactions on Management (ATM)*, *2*(2), 159–167.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352–375.