International Journal of Cyber and IT Service Management (IJCITSM) p-ISSN: 2797-1325
Vol. 2 No. 1 April 2022 e-ISSN: 2808-554X

Adoption Computerized Certificate Transparency and Confidentiality

Deden Rustiana[1], Julysar Diti Pratama[2], Taufan Mudabbir[3], Muhamad Ali Fahmi[4], Galih Ahmad Rofei[5]
University of Raharja[1,2,3,4,5]
Jenderal Sudirman No.40, Cikokol, Kota Tangerang[1,2,3,4,5]
Indonesia[1,2,3,4,5]
e-mail: deden.rustiana@raharja.info[1], julysar.pratama@raharja.info[2], taufan.mudabbir@raharja.info[3], ali.fahmi@raharja.info[4], galih.ahmad@raharja.info[5]

Author Notification
April 2022
Final Revised
April 2022
Published
April 2022

To cite this document:
Rustiana, D., Pratama, J.D., Mudabbir, T., Fahmi, M.A., & Rofei, G.A. (2022). Adoption Computerized Certificate Transparency and Confidentiality. *International Journal of Cyber and IT Service Management (IJCITSM)*, *2*(1), 1-10. Retrieved from https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/65

DOI:
https://doi.org/10.34306/ijcitsm.v2i1.65

Abstract

Due to the unavailability of issuing entities, the increasing number of valuable documents that are still being issued in printed form has an impact on forgery and cannot be verified. Academic certification is an achievement that everyone desires because it has a positive effect and has a continuity in their social life. These activities are listed as being able to identify, analyze, and try out any of the ledger options that are available. arise to provide greater efficiency, reliability, and a level of independence. By implementing a prototype that could issue, verify, and distribute certificates, the fact of the concept was proposed. The experimental test results are given, as well as the use of blockchain technology for the purpose of analyzing. Finally, this work outlines the current growth and maturity of equipment encountered, reports progress and limitations, and reveals issues that still need to be addressed.

Keywords *: Blockchain Technology, Digital Certificate, Blockcert, Transparency*

1. Introduction

In order to present the efficacy of blockchain technology, analysis of use in the field of education in producing and verifying degrees at universities. This is a continuation of work originally proposed in 2019 at the international conference "Network-based Distributed Computing and Knowledge Discovery (Cyber C)" [1]. Academic certificates ensure the certificate holder's expertise and are internationally recognized [2]. The skills that a person

Copyright © 2022 Deden Rustiana, Julysar Diti Pratama, Taufan Mudabbir, Muhamad Ali Fahmi, Galih Ahmad Rofei.
This work is licensed under a Creative Commons Attribution 4.0 (CC BY 4.0)

needs have a big effect on the income and social status of developing and developed countries. For example [3], in Brazil, information from the Pesquisa Nacional by Government - issued identification Domicilios Amostra (PNADC) shows if the level of education ensures the inclusion of Brazilians [4]. According to the results presented, the income of people who have completed a major education is almost three times that of people with only high school education. According to data from Eurostat1 in Europe, there are more than 2.5 million major education graduates in Europe each year. France and Britain are among the most respected countries, with over 370,000 graduates each year. The number of people aged 25 to 32 with a bachelor's degree nearly doubled in 8 years, from 23% in 2012 to 39% in 2019 [5].

When professionals have qualifications, broad understanding will be immediately replaced by income, so as to improve the quality of life. Not only that, these figures justify continued development and lay a solid foundation in the creation of solutions to verify the authenticity of university degrees. Due to COVID-19, the use of digital energy sources is very necessary in times of crisis, therefore the shortage of paper models is still widely used during the crisis, and this shortage continues to be real. Although there are digital plans to overcome this weakness [6], the solution still depends on the issuing entity to verify authenticity. From here, it's not just the innovation, blockchain is expected to share other improvements that digital solutions haven't yet achieved. Using the energy source required by technology can break the checking process of the publisher and always guarantee its authenticity. The second innovation relates to privacy. Certificates are documents that contain individual data and are sensitive to gaps in information security. If on the one hand it is necessary to protect student personalities, on the other hand it is profitable for the distribution of related personnel [7].

Lastly, loading a timestamp, compared to digital certificates, blockchain solving shares a third innovation. Because data cannot be replaced in chronological order and stored online, they can accurately reflect the exact date of the activity. Therefore, this article reviews the use of blockchain technology, with the aim of learning from academic certificates with this innovative possible way [8]. The benefits of the document organization are as follows: The following section briefly describes blockchain technology. Next, we present the main comparisons between blockchain cracking and digital certificates; after that, we present the CertEdu prototype raised by Fernando Pessoa University (UFP), as well as briefly review the results obtained, as well as the conclusions shared. Some of the final opinions made.

2. Research Methodology

One of the improvements proposed by blockchain confirmation game plans is disengaged check. For example, it is possible to affirm the validness of the endorsements, using a disengaged neighborhood copy. All supports that are presently there are totally obvious. Nonetheless, the model found that this part was not met, due to the way Blockcerts completes the affirmation cycle [9]. There is a dependence on two external records (encouraged by the underwriter's specialist), one for school recognizing verification, and another for checking confirmation forswearing. Concerning first dependence, Learning Machine and NextID in late 2019, conveyed an article with a suggestion to override the underwriter profile. This handiness ought to be accessible in variations 3.0 of blockcerts. Worried, there is still no legitimate response for the issue. The paper presents different approaches, for instance, sharp arrangements [9], control data or even the joint use of Interplanetary File System (IPFS) and blockchain [10].

2.1 Literature review

The solution was proposed by Zyskind et Navy (AL) meaning universal personal issues, such as ownership of information, transparency of information, audited features and detailed access controls. The solution is mainly concerned about the mobile platform access control management system as well as the user can not revoke the given access to his personal information. By installing a mobile application, the permission is granted without time limit, the user is obliged to do this if necessary, uninstall the application and stop using the service, revoke access. The purpose of this new solution is to provide the user with the expertise to control and audit what information is stored and how the methods of storing it are used. As previously stated, mandatory access rights can be revoked. Therefore, the technical inspiration is to maintain a policy of access to private information. After that, moderate the blockchain nodes. Access to DHT (Distributed Hash Table).

In another paper by Gupta et al. [11], explained that the final owner can personally own the data and provide the necessary authorization to access it. You can even encode smart contracts as blocks containing related insurance, emergency contacts, wills, smart contracts to be activated by this program Blockchain can be seen from other website services. Through blockchain, digital products can be operated and provide privacy security in sharing healthy consumer health records.

2.2 Blockchain

This technology is already attracting people's attention via the Bitcoin cryptocurrency and is soon growing in several other applications. There are 3 types of blockchains: public, private or consortium [12]. Blockchain is a distributed system consisting of notes arranged in blocks and linked to each other via cryptographic mechanisms. Public networks, also known to be like blockchain without permission, provide a free access area for every participant who wants to join the network. However, the transaction verification conditions have been set and cannot be changed by other members. Generally, this type of blockchain employs a Proof of Work (PoW) consensus mechanism. In a network of individuals, known as a licensed blockchain, provisions stem from business interests. The organization controlling the network can determine, for example, which users want to determine consensus, or how to administer the network to recruit new members. In conclusion, a consortium network is a type that mixes public and individual network attributes in the same area. For example, in some cases, it would be interesting to maintain public access to the network, but some information can also be encrypted to protect the privacy and anonymity of participants.

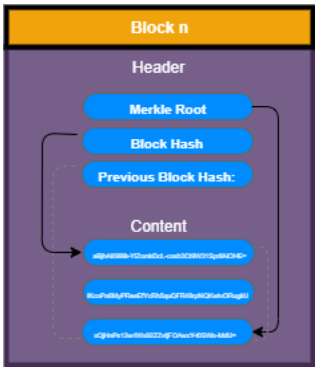

Fig 1. Universal Reflection of Block Structure

For example in Figure 1, the use of transactions is to transfer assets from one account to another. The owner of the asset can move it to the blockchain via an account identified by a public address, which is monitored by a matching individual key . There is a conceptual comparison between the public key and the public address. The public key is used to confirm the signature made by the private key owner, when identifying an account an address is required. Taking Bitcoin as an example, the process of creating an address is something like this: the public key is obtained using the digital signature algorithm (ECDSA) function to curve the elliptic to individual keys; public key has 2 benefits, Secure Hashing Algorithm (SHA) - 256 and ethnic integrity Primitives Evaluation Message Digest (RIPEMD) - 160; By passing the Base58 Check function, the dimensions of the result string can be reduced to obtain an address, such as mgAzKQZZi47g4UMvmGJCsicbJ4P3B8S HRr [13].

2.3 Certification

Compared to the paper model, digital certificates are quite innovative, but they cannot guarantee verification and sharing because they rely on a central point. As Schar pointed out, academic certificates can be useful if they can be validated. This article improves the implementation of blockchain technology in each process, especially in terms of validation and sharing. The certification process links 3 things, namely sharing, validation and publication [14]. The technology that disrupts blockchain is that it allows the creation of structures capable of carrying out independent verification processes. shows a typical scenario linking universities, students and entrepreneurs. Please note that Jane's certificate can be verified directly on the blockchain without having to go through a university [15].

Table 1. Comparison between electronic certificates vs. blockchain solution

Property	Advanced certificate	Blockchain certificate
Excellence	Relying on advanced signatures	Part of the encryption used
Personal	All information is available in the certificate	Only the hashes are public
Autonomy	Depends on central governing body	Technology changes third party intermediaries
Missing information	Relying on backup mechanisms	Standard normal distribution
Proof of existence	Date subject to customer suitability	Timestamp represents fact date

Table 2. Comparing among analyzing tools

Qualification	BTCert	Hyperledger	EduCTX	Blockcerts

Blockchain Agnostic	❌	❌	❌	✅
Only the Lord of Identity	✅	✅	✅	✅
Active user organization	❌	✅	❌	✅
Registered internet	✅	❌	❌	✅
Personal matters	✅	✅	✅	✅

The use of hashes can log certificates directly on the network, so that no individual data can be retrieved from Jane. This can be intertwined because public data on the blockchain has no impact on students. In conclusion, Jane has the autonomy in providing digital certificate documents with whoever she wants, and each recipient of these documents can see their own validation on the blockchain. Blockchain innovation is seen in many aspects. Technology feels more comfortable, because it is not like a digital certificate, the whole certificate security depends only on the digital signature, the use of a different encryption mechanism, combined with the use of a distributed big novel, can provide a greater level of certificate security.

Overwriting personal, keep in mind that if the certificate contains all individual data, digital certificates are more vulnerable to information security. In fact, this can get in the way of its reproduction. After sorting out this equipment in the blockchain cracking process, the data transmitted has no impact on the student, and the certificate can be issued without anxiety. Digital signatures rely on a central authority. In some countries, moreover, there is no institution capable of authenticating the signal. In this case, blockchain technology provides complete autonomy, thereby eliminating third -party intermediaries. The most important in blockchain is the field of public architecture as well as the consortium, providing a native backup mechanism because it copies all data simultaneously. On the other hand, digital certificates are easily destroyed electronically and rely heavily on extra powerful mechanisms to avoid losses. Lastly, with regard to the fact of existence, the expertise in the accuracy generated by the digital certificate depends on the sub -scribe's expertise. blockchain allows timestamps to be recognized. This can be a problem, if the individual university keys are confiscated and the thief uses it to sign the certificate, coinciding with the validity of the certificate returning to coincide with the theft being reported. In this case, the blockchain allows timestamps to be recognized. As Ronning put it, "All credentials issued using stolen keys must run aground".

3. Results and Discussion

In actuality, Blockcerts was the solitary testament giving arrangement that was brought into the world with the necessity to work for any blockchain. This prerequisite enormously builds the multifaceted nature of the arrangement, however it is significant in light of the fact that it keeps the application life cycle long. Another point that drew consideration is its dynamic

network of engineers, which causes the venture to get steady updates. Intriguing focuses were additionally noted on different stages. BTCerts, an undertaking roused by the MIT arrangement, addresses the issue of unifying the disavowal cycle of Blockcerts. The model proposed by BTCerts settles the issue and can be handily adjusted to a blockchain, yet the expenses are concernedly, predominantly on the grounds that it doesn't clarify how the correlative denial data would be enrolled, since the OP RETURN DATA field has a restricted size of 83 bytes.

3.1 Prototype

UFP has assembled a model and has been trying the machine of instructive endorsements with blockchain innovation. The machine called CertEdu was constructed to support the Blockcerts stage and has its engineering planned by the figure 5. As you will see, CertEdu issues electronic archives on Bitcoin and Ethereum networks. The objective of executing two organizations is decisively to survey the model's capacity to comprehend the required blockchain similarity property. The usage depicted during this work shows that in any event, existing alternate approaches to figure the blockchains (permissioned, permissionless, consortium), the actualized arrangement is surely adjusted to figure on any sort of organization on account of these reasons the arrangement utilizes its own Merkle Proofs system, the procedure of mooring the certificate hash on the blockchain, permits check and defeats the space restriction, the arrangement needn't bother with the utilization o f brilliant agreements The specialized norm of Blockcerts was intended to work with any blockchain, hence keeping the achievement of the task from being molded to the advancement of another item. In 2017 when the task was begun, incorporation was just conceivable with Bitcoin, however it before long reached out to Ethereum. In 2018, Universidad del Rosario, in Colombia, constructed the mixing with Hyperledger. Blockcerts utilizes various layers that business together to shape the hashes for each clump of authentications, giving them on the blockchain and in this way permitting web stages to print the endorsements by utilizing JavaScript Object Notation (JSON) protests and checking them on the blockchain. The figure 3 shows a cycle of making a computerized authentication on the blockchain by utilizing the parts of Blockcerts. As we'll see, the resource put away is the hash of the JSON created document, which is practically speaking methods connecting the advanced record with the blockchain. The following area depicts CertEdu usage. Cert-apparatuses are subject for making the declaration layouts which will later be marked and secured on the blockchain. for each model, it's conceivable to tweak data like the title, logo, description, history. There likewise are adjustable fields, all together that particular data are frequently treated. These fields are frequently made all around the world (they will show up for all the declarations produced from the model being referred to) or by the beneficiary (they will just show up for a chosen gathering of beneficiaries). Next, a piece of the code of communication with the segment is introduced.

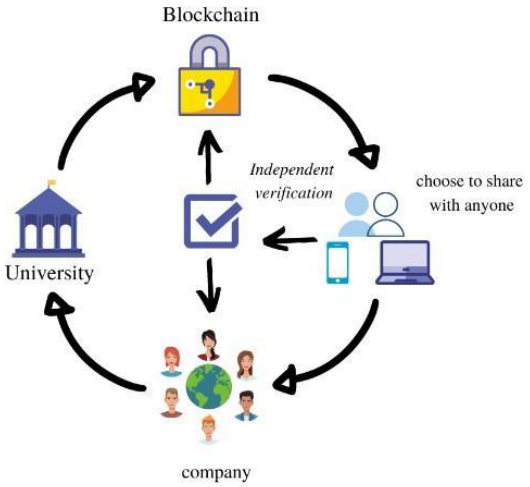

Fig 2. CertEdu Certificate Template

Cert-tools receives as an input the knowledge which will form the certificate and as output, returns a file JSON, able to be signed by subsequent components. The enter question is generated by a Block certs module called cert-schema 4, which is predicated on the Verifiable Credentials (VC)5. The info types mapped by the quality follow the norm Internationalized Resource Identifiers (IRIs), an equivalent employed by XMLSchema 6. All this concern in following these standards is to supply entities and interested parties a uniform format for certifications. The figure 4 shows the implementation of cert-tools in CertEdu. The model stored within the database contains the required parameters for the issuance of a certificate. In another system interface, all it takes is to link the model code with an inventory of scholars so as to publish the certificates. Note that there's a standing indicator, which checks when saving the record if all settings are applied successfully. For instance, there's a parameter that permits you to point to the general public address of the certificate. When it's activated, the appliance tries to publish on the indicated website with the parameterized access credentials. If it fails, the model remains pending and can't be used until the error is fixed.

3.2 Publishing area

Cert-backer is the part answerable for creating the transaction on the blockchain. The information gets the certificate record created by cert-devices and returns as yield the confirmation hash distributed on the blockchain. Its job, notwithstanding the marking, is to permit blockchain similarity, by giving a structure that permits connectors from different organizations to be executed. In the part territory called blockchain overseers, everything necessary is to make three capacities to connect another organization: association (connectors.py), (exchange handlers.py), and supporter (signer.py). In addition, it is important to change the square beneath the principle capacity of the part.

The standard is kept up by the open-source network, to help networks the Bitcoin and Ethererum. The joining to different organizations is arising as activities do, for example, the University of Rosario, in Colombia, which constructed the connector for Hyperledger, and is trying it tentatively. Another prominent purpose of the figure 3 is the chance of marking a gathering of models immediately. In fact, cert-instruments produces a few testament documents and computes the gathering's Merkle root, recording this incentive on the blockchain.

The figure 6 shows the structure of an endorsement document that makes up a bunch. All records in the bunch have a similar incentive as the Merkle Root field, and furthermore

store, notwithstanding the hash itself, the hashes of the hubs expected to check the foundation of Merkle (verification 0, 1 and 2 of 6). Practically speaking, when the verifier gets a document, it computes the hash and minds the blockchain whether this record has a place with the produced clump. With that, you just need to invest a solitary energy, to be conceivable to check n testaments. Additionally, this check is extremely valuable for denial, on the grounds that dropping a solitary blockchain enlistment naturally drops the whole group.

3.3 Embedded Authenticity Checker

The verifier has two jobs: to educate the realness regarding an authentication and to speak to it graphically to the client. The main variants of this segment in Blockcerts were called cert - watcher, however later changed to blockcerts-verifier 8. The innovation depends on JavaScript, which makes it simpler for applications, for example, CertEdu, to set out on a widespread declaration verifier inside its structure. How the issuance cycle is executed, straightforwardly impacts on the multifaceted nature of actualizing this segment. Prominently, Block certs tries to utilize normalized segments of the blockchain, for example, hashes, exchange recording, and Merkle root. With this, the inclusion of new blockchain in the activity of the blockcerts-verifier turns into a less complex cycle. Thinking about an alternate situation, in which the systems utilize brilliant agreements, contingent upon the manner in which it is actualized, this cycle of fusing new organizations can get intricate. There is still no characterized standard on the showcase configuration of the advanced endorsement (figure 7 and 8). In spite of the fact that this is certifiably not a specialized security issue, it can cause some doubt for an appraiser who gets a similar certificate given by a similar telecaster however in various configurations. Luckily, the check capacity can ensure the information veracity to the invested individual, and can even approve the document in various all inclusive verifiers, for example, the one offered by Blockcerts 9.

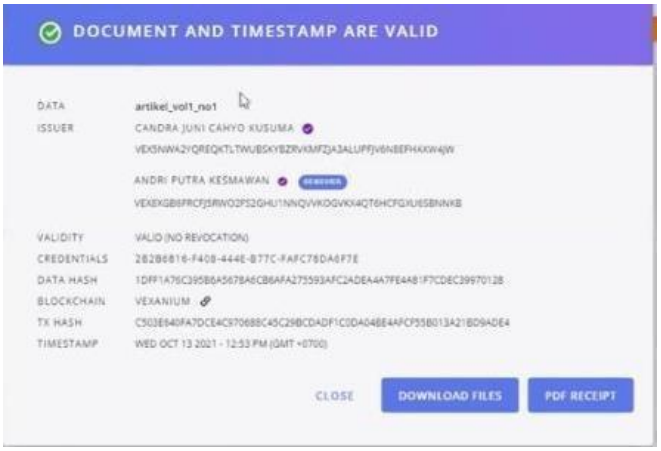

Fig 3. Model 1 for viewing a digital certificate issued by Blockcerts

4. Conclusions

Recognition extortion is a path from being finished. The battle systems end up being amazingly wasteful, for the most part inside the paper models. Computerized degrees have advanced with digitalization, however they do not offer security to the researchers, all together that they can put stock in openly disseminating their declarations. Blockchain's problematic innovation offers a discovery in circulation and guarantees assurance from altering. It has been likewise indicated that the blockchain offers the least complex assets to act simply in the event of misfortune or robbery of the college's private key, ensuring the

substance against unnecessary retroactive outflows. Plus, the degree of protection offered by the innovation, by recording just the hash testament on the blockchain, makes the appropriate response less powerless to information spillage than the advanced endorsement arrangements without blockchain. The emergence of the objective of utilizing the blockchain for the administration of confirmations was accomplished during the development of the CertEdu model, during which it had been conceivable to work issues, disavowals, offers, and checks of instructive endorsements. In any case, tests likewise recognized that disengaged activity remains a difficult problem that should be dealt with. Albeit some blockchains effectively offer assets, similar to the savvy contract, which may permit to just determination the centralization focuses put, the reason of the appropriate response working on such a blockchain has not been met, so those issues that likewise forestall decentralization are as yet raised by this work is forthcoming. There is additionally worry about the eccentricism of the issuance costs. Considering public organizations like Bitcoin and Ethereum, you can't foresee the speed of exchanges inside the day's end. This issue can repress the attachment of colleges. At long last, it's inferred that the machine of blockchain inside the administration of instructive declarations is totally conceivable which the innovation as of now offers benefits regarding security, appropriation and repudiation, contrasted with advanced arrangements. In any case, to be prepared to capitalize on the total capability of the innovation, the centralization focuses tended to by this work, similar to the approval of the guarantor's profile and denial, had the opportunity to be relocated to highlights that work inside the blockchain itself.

References

[1] C. Lukita, M. Hatta, E. P. Harahap, and U. Rahardja, “Crowd funding management platform based on block chain technology using smart contracts,” *J. Adv. Res. Dyn. Control Syst.*, vol. 12, no. 2, 2020, doi: 10.5373/JARDCS/V12I2/S20201236.

[2] L. Chandra, Amroni, B. Frizca, Q. Aini, and U. Rahardja, “Utilization Of Blockchain Decentralized System In Repairing Management Of Certificate Issuance System, ” *J. Adv. Res. Dyn. Control Syst.*, vol. 12, no. 2, pp. 1922–1927, 2020, doi: 10.5373/JARDCS/V12I2/S20201235.

[3] C. Wright, R. Caudy, D. R. Kent IV, H. Bronnimann, and R. Teodorescu, “Computer data system data source refreshing using an update propagation graph.” Google Patents, Feb. 25, 2020.

[4] D. Immaniar, N. Azizah, D. Supriyanti, N. Septiani, and M. Hardini, “PoTS: Proof of Tunnel Signature for Certificate Based on Blockchain Technology,” *Int. J. Cyber IT Serv. Manag.*, vol. 1, no. 1, pp. 101–114, 2021.

[5] 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, 2021.

[6] U. Rahardja, A. S. Bist, M. Hardini, Q. Aini, and E. P. Harahap, “Authentication of Covid- 19 Patient Certification with Blockchain Protocol.”

[7] E. Uprichard and L. Dawney, “Data diffraction: Challenging data integration in mixed methods research,” *J. Mix. Methods Res.*, vol. 13, no. 1, pp. 19–32, 2019.

[8] M. Yeni and D. Kumala, “Teknologi Blockchain untuk Transparansi dan Keamanan pada
Era Digital,” 2020.

[9] F. P. Ramos and M. Sperandio, “9 The Impact of Translation Competence on Institutional Translation Management and Quality,” *Institutional Transl. Interpret.*

Assess. Pract. Manag. Qual., p. 174, 2020.

[10] M. Ez-Zaouia, A. Tabard, and E. Lavoué, "Emodash: A dashboard supporting retrospective awareness of emotions in online learning," *Int. J. Hum. Comput. Stud.*, vol. 139, p. 102411, 2020.

[11] B. Setiawan and S. De Lagarde, "EDUKASI BLOCKCHAIN SEBAGAI SOLUSI BISNIS MASA DEPAN BAGI PELAKU USAHA MIKRO, KECIL DAN MENENGAH (UMKM) DI KOTA PALEMBANG," *J. Abdimas Mandiri*, vol. 3, no. 2, 2019.

[12] M. Yusup, Q. Aini, D. Apriani, and P. Nursaputri, "PEMANFAATAN TEKNOLOGI BLOCKCHAIN PADA PROGRAM SERTIFIKASI DOSEN," in *SENSITIf: Seminar Nasional Sistem Informasi dan Teknologi Informasi*, 2019, pp. 365–371.

[13] H. F. Putra, W. Wirawan, and O. Penangsang, "Penerapan Blockchain dan Kriptografi untuk Keamanan Data pada Jaringan Smart Grid," *J. Tek. ITS*, vol. 8, no. 1, pp. A11– A16, 2019.

[14] Y. P. S. Balhara, D. Kattula, S. Singh, S. Chukkali, and R. Bhargava, "Impact of lockdown following COVID-19 on the gaming behavior of college students," *Indian J. Public Health*, vol. 64, no. 6, p. 172, 2020.

[15] I. Isma, "Sistem Sertifikasi Halal Pada Rumah Potong Hewan Dengan Menggunakan Teknologi Blockchain." UNIVERSITAS AIRLANGGA, 2020.