



Journal of applied research and technology

ISSN: 1665-6423

Universidad Nacional Autónoma de México, Instituto de
Ciencias Aplicadas y Tecnología

Rahardja, Untung; Hidayanto, Achmad Nizar; Putra, Panca Oktavia Hadi; Hardini, Marviola
Immutable Ubiquitous Digital Certificate Authentication Using Blockchain Protocol

Journal of applied research and technology, vol. 19, no. 4, 2021, pp. 308-321

Universidad Nacional Autónoma de México, Instituto de Ciencias Aplicadas y Tecnología

DOI: <https://doi.org/10.14482/INDES.30.1.303.661>

Available in: <https://www.redalyc.org/articulo.oa?id=47471703003>

- How to cite
- Complete issue
- More information about this article
- Journal's webpage in redalyc.org

UNAM redalyc.org

Scientific Information System Redalyc

Network of Scientific Journals from Latin America and the Caribbean, Spain and
Portugal

Project academic non-profit, developed under the open access initiative



Immutable Ubiquitous Digital Certificate Authentication Using Blockchain Protocol

Untung Rahardja^a • Achmad Nizar Hidayanto^b • Panca Oktavia Hadi Putra^b • Marviola Hardini^{a*}

^aUniversity of Raharja, Banten, Indonesia

^bUniversity of Indonesia, Jawa Barat, Indonesia

Received 05 30 2020; accepted 04 20 2021

Available 08 31 2021

Abstract: A new paradigm regarding a significant technological development has been introduced, each individual gets full trust in controlling an asset and can see the level of authenticity of a particular asset. Through qualitative methods, it is possible to have structured results as the first step to the perfection of the digitalization era, in which the current revolutionary technology called blockchain has come into play. One of the main innovations found through this research is the role of blockchain in enhancing e-certificate data security, it is proven that administration can be well distributed and reduce operational costs for every field in the world. It is clear that blockchain, especially in the world of education certification, has a big impact, because it can create a global trust network, immutable, authenticated, ubiquitous, and can shape a better world for Indonesia as a superpower. With good execution using the SHA-256 hash, e-certificate blockchain technology can be of high value and have an impact on the quality of potential human resources in educational institutions.

Keywords: Blockchain, E-Certificate, Educational Institution

*Corresponding author.

E-mail address: marviola@raharja.info (Marviola Hardini).

Peer Review under the responsibility of Universidad Nacional Autónoma de México.

1. Introduction

One of the world's most revolutionary technologies has been discovered, known as the blockchain, a disruptive platform that transforms many aspects of life (Ensmenger, 2018; Skinner, 2016; Whyte, 2019). Every individual needs to focus on understanding the science of blockchain, because basically the use of blockchain technology has high potential to change various industries in various ways (Beck & Müller-Bloch, 2017; Rahardja, Bist, et al., 2020).

Blockchain is a ledger of decentralized digital transactions without control by individuals, groups or companies, so that the data structure that has been available cannot be changed (Mattila, 2016). Because if the information submitted is wrong it will cause problems. Databases can only be added without being deleted so that each transaction will be summarized into a new block that continuously forms a chain, this eternity makes the blockchain different from ordinary databases (Bergstra & Burgess, 2018; Sunarya et al., 2020).

Various industries, businesses and even governments have been captivated by the charm and sophistication of blockchain technology, with a transparent transaction database also distributed. In particular the financial industry which initially rejected blockchain technology, is now beginning to learn to understand how the system works and the impact of the blockchain (Peters & Panayi, 2016; Teece, 2010).

A thorough Bibliometric Analysis and Review of 387 blockchain research has been conducted, and the six most popular keywords were found, including 66.7% regarding Smart Contract, 11% regarding Ethereum, 8.8% regarding Distributed Ledger, 6.7% regarding Crypto-currency, 4.8% regarding Security, and 2% regarding the Supply Chain (Ante, 2020). The remaining subject interests are relatively insignificant in terms of research attention given by the world blockchain scientists. It caught us by surprise how few have given any attention to blockchain application in education. Like other economic sectors, looking at the challenging problems facing the education sectors, blockchain technology presents the most potential to solve current issues and leapfrog to a new way how education could be conducted like never before. We are all aware that this can only happen if many scientists collaborate on innovation and scientific discoveries on using blockchain technology in the education sector. Mexico already launched blockchain pilot programs for Mexican specific elementary schools (Franzoni et al., 2019). This research aims to achieve similar or better results for Indonesian specific implementation in tertiary education.

The focus is on greater attention to building blockchain applications to enhance learning objectives and increase competency attainments and personal information securities in the educational sectors (Alammary et al., 2019).

Therefore, the world of education also does not want to be left behind by today's sophisticated technology, where blockchain can be adopted by educational institutions, especially in profiling each individual with the final result in the form of a certificate in digital form equipped with blockchain sophistication (Rahardja et al., 2019). This is necessary because of the prevalence of falsification of diploma data in educational institutions in Indonesia, so the quality of Human Resources (HR) is questionable. This study confirms that information distribution activities can be controlled and personalized properly using blockchain-based digital certificates which have a significant effect on public satisfaction and data security (Hariguna et al., 2019; Rahardja & Raharja, 2009).

The novel contribution mainly emphasizes exploiting blockchain technology in the education sector within Indonesia. There are still many internet connectivity problems in rural areas and towns through Indonesia's educational institutions' geographic distribution. Even though they have implemented a server system in the ministry in urban areas, they still rely on local servers in their respective institutions. The existing data management still applies to a single server database. And according to the Three Tier Architecture or better known as the Client-Server Programming concept, it requires the availability of a User Interface that can facilitate clients, flexibility in access to servers and databases because the work is carried out separately without any influence from other layers. If additional features can be done coordinatively in each existing layer, this can be beneficial in creating and developing a secure application. In that case, the data is more resistant to security hacks so that the authentication of every processed information is guaranteed, and usability utilization becomes robust.

Figure 1. A study was made in which the results of profiling to be included in the certificate need to be encrypted so that it has 2 keys to be able to open it, namely public key and private key (Komputer, 2013; Muzayana et al., n.d.). Then the key needs to be applied also hashing so that the certificate cannot be falsified by irresponsible parties (Heriyanto, 2016). Blockchain in a certificate can be used to determine the validity of data (Yusup et al., 2018). As well as reducing the burden of monitoring an admin to maintain the stability of data security that is vulnerable to problems (Nurhaeni et al., 2019).

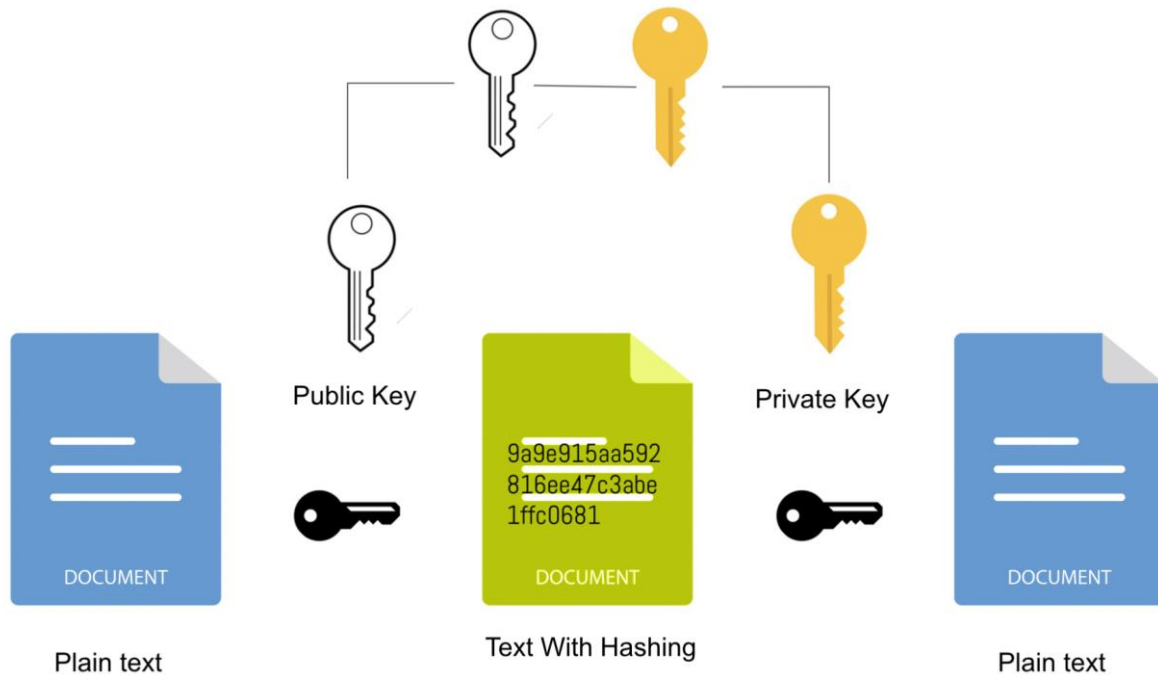


Figure 1. Public Key and Private Key.

2. Research Methods

Qualitative research methods were adopted in this study, there are three approaches such as literature review, case studies, and library research to produce research evidence (Guritno & Rahardja, 2011). With the advent of blockchain technology, the qualitative method presents a pragmatic approach in involving current technology in the initial stages.

Despite the rapid development of cloud computing technology, security and trust in data is still a major challenge (Wei et al., 2020). Problems that are present in the future will be increasingly challenging for higher education. Especially regarding the validation of documents that require a new revolutionary tool (Lizcano et al., 2020). Apart from the increasing interest in blockchain, which is still classified as a new topic, research is being conducted to introduce better blockchain, especially in the field of education (George et al., 2019). Over time the evolution of research has resulted in major discoveries and has been done through detailed analysis (Dabbagh et al., 2019). Where has been carried out a survey of smart communities who independently use a revolutionary technology as a key component (Aggarwal et al., 2019).

The level of information security and data transparency can be improved through a technology called blockchain, because it is ensured to have high integrity in achieving the

confidentiality of records or data (Lee, 2019; Pal et al., 2019). Immutable code can be used to prevent undetected updates from data or information that has been stored in an agency database (Liu et al., 2017). Then the encoding rules for mapping information sequences using immutable code also need to be applied (Aini et al., 2020).

In addition to using immutable code, seeking ubiquitous technology can make security more complex and more difficult to solve (Sellami et al., 2019). In the problems that arise at this time, educational institutions are so rampant, open and ubiquitous, so that professionals at the company need time to be able to validate every prospective new employee (Lizcano et al., 2020). To make transactions or transfer data securely, authentication is the main thing in order to help the network reduce illegal users and prevent fraud. Because the data authentication process effectively identifies users well. So that the authentication process that will be performed can prevent security attacks on user data (Rahardja, Hardini, et al., 2020).

Quoted from WoS from 2013 to 2018, studies show that researchers have changed their research interests from Bitcoin to Blockchain in the past two years. There are four fields of research, namely Computer Science, Engineering, Telecommunications and Business Economics, where most papers or research scientific papers cover Blockchain technology (Mohammed et al., 2020). Blockchain keeps a

permanent record and transaction history, but nothing is truly permanent. Immutable blockchain records are based on immutable networks. In the context of the blockchain, it means that most members of the blockchain community must agree to change information and incentives not to change data (Laurence, 2019).

Through blockchain technology, facilitates the development of equipment and great trust, where an authorized party needs to ensure the quality of secret codes as a method of data security (Zeng et al., 2019). Although the main role of decentralized ledgers, such as blockchain, is storing data related to interactions between users to build trust, that is not enough, because blockchain technology has the possibility to offer better functionality and sophisticated quality (Hu et al., 2018).

Nowadays mesh networking and blockchain are the two hottest technologies in the telecommunications industry. Combining the two technologies can produce a new formula again regarding internet access. Mesh networking makes connecting to the internet easier and more affordable, when the blockchain merges in mesh networking technology, making internet access increasingly high selling points by enabling sharing of bandwidth for crypto-tokens (Selimi et al., 2018). Besides the blockchain technology is also proposed as a coordinating tool to support the non-monotonic consistency requirements of the IPFS system, because IPFS presents a peer-to-peer system that allows data distribution through the internet network (Tenorio-Fornés et al., 2018). Where all the popular companies engaged in blockchain technology use the Elliptic Curve Digital Signature Algorithm (ECDSA) (Durand et al., 2018), and so the hidden novelty and benefits of blockchain technology can serve as a tool for designing smart cities and social structures. The greater use of blockchain technology, the possibility to have a new mode of social organization will also increase (Swan, 2018).

Blockchain technology also has the potential to be able to contribute in various fields, where the application of blockchain technology in the energy and industrial sectors has been successfully carried out, but there has been no application in the education sector specifically in the certification section (Brilliantova & Thurner, 2019; Hughes et al., 2019). If certificates in the world of education can be embedded with blockchain technology optimally, then educational institutions can improve the quality of data security and the level of originality of the data held.

But the use of blockchain technology to track physical assets is not new. Technology that can track products used to be based on an RFID chip, one limitation is scalability with regard to the number of transactions that can be processed by the network. This can be overcome by protecting and monitoring using unique patterns. Using a hash that can ensure data privacy, timestamp is also a consideration as

evidence of the existence of immutable data, with this approach, the integrity of data tracking cannot be contested (Hepp et al., 2018).

So, it can be concluded through previous research, that knowing the features of blockchain technology in depth can have an effort to show how the blockchain can be programmed and implemented for many people is not limited to cryptocurrency (Singhal et al., 2018). Because in practice in the world of education the community also takes part in requiring a high level of security to be able to maintain privacy and the level of originality of a certification.

2.1. The Accuracy of The One-User Verification Process

With the validation stage using public keys and predefined parameters to calculate the verification equation, it can be concluded that the integrity of the data is damaged. In the case of complete data, the parameters do not change, and the left and right sides of the verification equation are calculated respectively.

Equation from the left side:

$$\begin{aligned} e(\sigma, g) &= e(\prod_{i=1}^{r_c} e_i^{\omega_i}, g) = e(\prod_{i=1}^{r_c} (h(f_i).a^{f_i})^{k.\omega_i}, g) \\ &= e(\prod_{i=1}^{r_c} (h(f_i).a^{f_i})^{\omega_i}, g) = e(\prod_{i=1}^{r_c} (h(f_i)^{\omega_i} \cdot \prod_{i=1}^{r_c} a^{f_i \omega_i}, g) \\ &= e(\prod_{i=1}^{r_c} (h(f_i)^{\omega_i} \cdot a^{\sum_{i=1}^{r_c} f_i \omega_i}, b) \end{aligned}$$

Equation from the right side:

$$= e(\prod_{i=1}^{r_c} (h(f_i)^{\omega_i} \cdot a^{\mu}, b) = e(\prod_{i=1}^{r_c} (h(f_i)^{\omega_i} \cdot a^{\sum_{i=1}^{r_c} f_i \omega_i}, b)$$

Proof:

$$= \{\mu, \sigma, (h(f_i)_{1 \leq i \leq r_c})\}$$

It can be seen that the equation is the same on both sides. Since parameters a and b are both publicly available, only if the parameters in the formula are changed, there will be an imbalance between the two ends of the equation, and cloud server-side data can be changed. Therefore, by determining the balance of the equation, it is determined whether the data integrity is still intact.

3. Results and Discussion

Blockchain employs some smart incentives to maintain honest agencies, this is to ensure the stability of the network now and in the future.

Blockchain-based certificate units are based on proof of work, which requires the expenditure of time and energy by each agency that must obtain, manage and operate a blockchain-based digital certificate engine.

Figure 2. Where each certificate transaction (CTx) will be tested whether it is considered valid. Transaction is valid if it follows the rules and according to the structure, if multiple transactions are considered invalid. In addition to conveying these valid transactions, some nodes also provide computing

power to the network by putting all valid transactions they receive into blocks. Where each block arranged linearly is called blockchain. The hash-based structure is one of the most promising candidates to be used in this study because it can help certificate data security (Ma et al., 2020). Operational patterns and file behavior can be monitored based on timestamps so that they can be recorded in the ledger for each block transaction that is carried out (Ho et al., 2018). Nonce itself is a method of generating random values that can be used for authentication, most nonce-based authentication schemes require verification tables that are stored on the server to store nonce in the next authentication session (Zainuddin et al., 2017).

Based on the current decentralized file system observation

capacity as a metadata statement about the existence of digital resources that cannot be changed in this study is called immutable. The Interplanetary File System (IPFS) as a basic example of supporting infrastructure with minimal convention sets, can be used as an alternative mechanism for storing byte streams in digital repositories such as DSpace or CKAN (Sicilia et al., 2019).

Ubiquitous technology is a contemporary innovation that significantly revolutionizes the way agencies are connected and interact with various stakeholder interests. Agencies can obtain user opinions regarding blockchain certificate services and can collect data about user behavior and habits. On the user side itself can have the advantage of accessing blockchain-based certificates anywhere, anytime without constrained access via mobile phones that are easy to carry anywhere (Margulis et al., 2020).

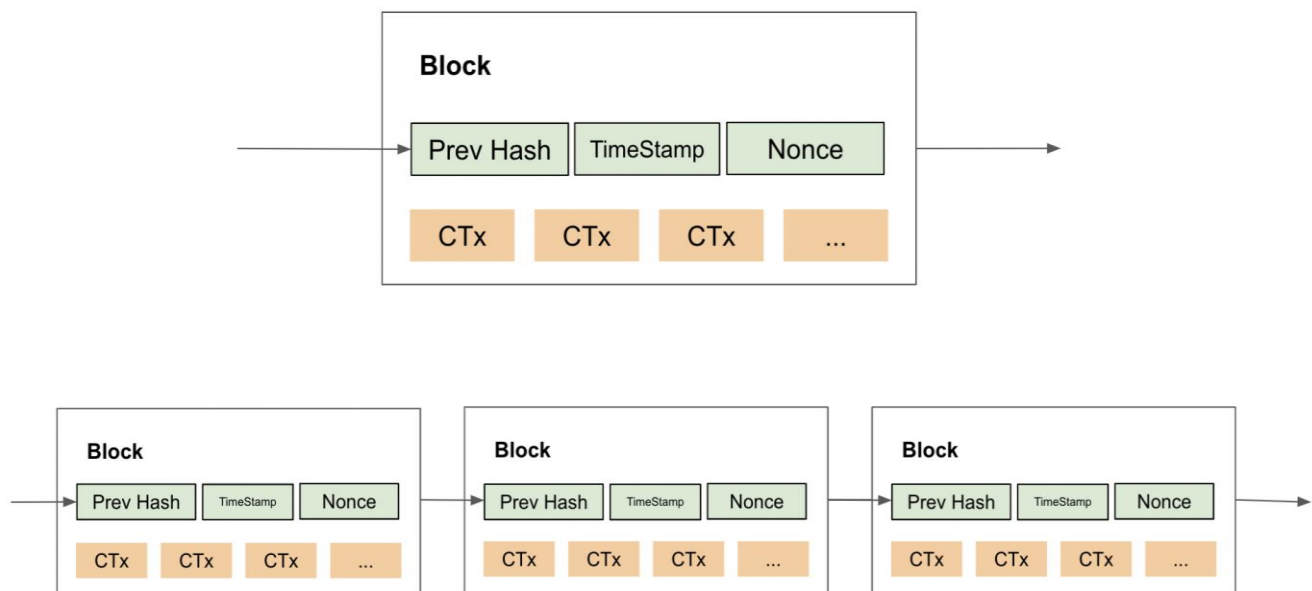


Figure 2. Blockchain Protocol.

3.1. Asymmetric Transmission

Something that is encrypted using a public key cannot be decrypted with the same public key or any key in the world, except with its private key pair. And something that is encrypted using a private key cannot be decrypted with the same private key or any key in the world, except with its public key pair.

Figure 3. Describes how Asymmetric Transmission works, there are 3 (three) key application methods with the best level of security located in the third method.

Because if we examine deeper in the first method, there are only a pair of keys to perform a data transaction. Allow illegal users to still be able to open scripts using the public key sender, which is published on the internet.

Another case with the second method, where the script is locked using the recipient's public key so that after the data is sent properly, the recipient's private key can only be opened. But this second method also has its own problems, where if there are illegal users who also listen to the plan between the sender and the recipient, then the illegal user can still

send texts containing different information. This explanation makes the second method safe, as well as ubiquitous, but the information received has not been authenticated and good.

Then a third method is made, where each user has a pair of keys called P: Private Key, and U: Public Key. It was explained that if you want to do a script, document or data transaction with other users, it requires a double level of security.

The first step of the sender is to lock a script that you want to send using the Public Key recipient that is obtained through the internet, then do security again using the Private Key owned by the sender. After the manuscript is sent, the way to open the manuscript is to use a Public Key sender that is retrieved via the internet, then reopened using a Private Key that is only owned by the recipient.

With the double security level as described above, each data transaction process will be assessed as Authenticated, Secure as well as Ubiquitous. So, the script can be sent to other users without worrying that other people who are not responsible can find out the contents.

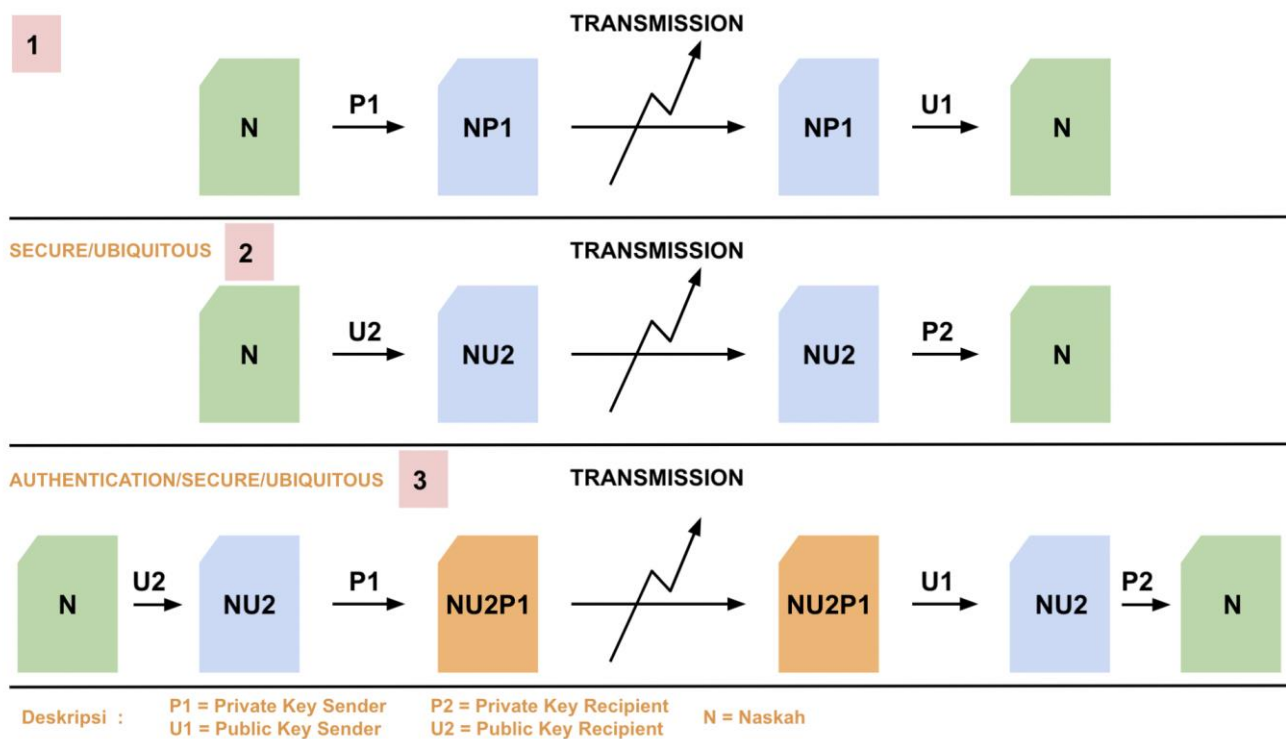


Figure 3. Asymmetric Transmission Blockchain.

3.2. Linear Coding System

```
<h2 id="1">SHA256 Encoder</h2>

<form id="hash_calculator"
method="post">

<label class="nostar"
id="label_hash_calculator_source_text"
for="hash_calculator_source_text"><input
type="radio"
id="hash_calculator_source_text"
name="source" value="text" checked> From
a character string</label><br/>

<label
for="hash_calculator_plaintext">SHA256
plain text or
password</label><br/><textarea
name="plaintext"
id="hash_calculator_plaintext"
class="mini">dCode</textarea><br/>

<label class="nostar"
id="label_hash_calculator_source_file"
for="hash_calculator_source_file"><input
type="radio"
id="hash_calculator_source_file"
name="source" value="file" > From a
file</label><br/>

<label
for="hash_calculator_file">File</label>

<input type="file"
id="hash_calculator_file" name="file"
style="margin-left:1em;" />

<span
id="hash_calculator_file_span"><span
id="hash_calculator_file_text">&nbsp;</span>
<a href="javascript:;"
id="hash_calculator_file_remove">[X]</a>
</span>

<input type="hidden"
id="hash_calculator_file_file"
name="file_file" value=""
autocomplete="off" /><br/>

<button
post="source,plaintext,file">Encrypt
</button>

</form>

<!-- advert -->
```

Explain how the process of changing encrypted data into 64-digit SHA-256 hash codes.

6KXeBs2QN9W46R2eZt4huMDsDlGRKxSJ2nfQEaR_SOE=

3.3. Research Result

Blockchain systems often use 'one-way' mathematical functions that map variable size data and vary into a fixed size data that is often referred to as a 'hash function'.

This study uses the SHA-256 hash function, where SHA-256 (256 bits) is part of the SHA-2 cryptographic hash function, designed by the US National Security Agency (NSA) and published in 2001 by NIST as the Federal Information Processing Standard AS (FIPS) (Adiyanto & Febrianto, 2020).

The SHA-256 Encryption Method has more substance compared to MD5, because basically MD5 is still vulnerable in dealing with collision attacks. Where in August 2004 at the annual cryptographic conference in Santa Barbara, California, a group of cryptographers succeeded in making two files with different content that have the same MD5 hash so that it is proof that MD5 can still occur a 50% probability of collision for MD5 there are still 2^{64} or $1,8 \times 10^{19}$ (Sudaryono et al., 2019).

A SHA-256 processor specifically, performs 64 iterations, more than 512-bit message blocks and 256-bit hash values are described as 32-bit, where hash messages consist of 256-bit lengths and contain a 64-hexadecimal digit code (Aini et al., 2019). For that data security system which is considered to have optimal substance is recommended to use the SHA-256 hash (Guustaaf et al., 2020; Maulani et al., 2020).

Figure 4. Explain that the blockchain-based digital certificate needs to be embedded with a QR Code whose source is the processed code or a private key. This is needed for a more optimal level of network or data security.

Figure 5. Where each profile data that has been converted into a certificate is then made into a hash code, a QR Code and a digital signature on a certificate are also embedded. Then generated a digital certificate based on the blockchain protocol.

However, something like a certificate that is given a QR Code and used as a hash, and even then, cannot be a picture of a blockchain protocol that works well, because basically if a hash has been embedded into a certificate, then the certificate is used as a hash again, then will produce a different combination of hash codes.

So, this research produced another method to keep embedded blockchain technology in the certificate. Where a certificate that has been created, needs to be check certificate from a hash.

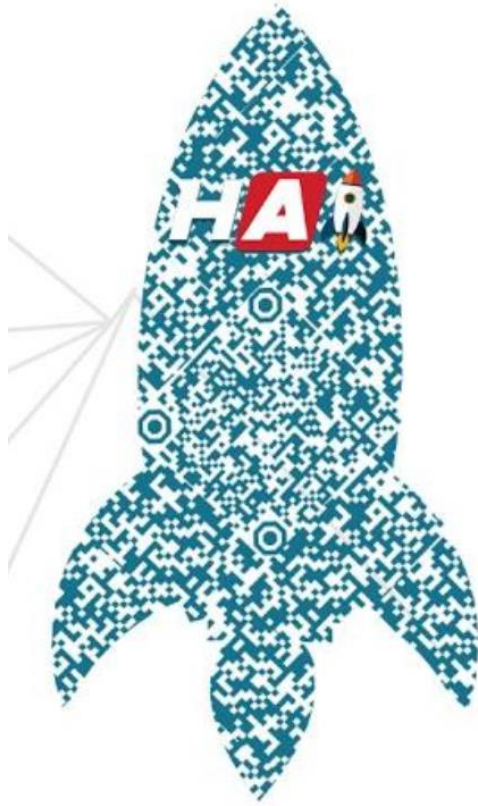


Figure 4. QR Code Blockchain Certificate.



Figure 5. Alphabet Incubator Blockchain Certificate.

Figure 6. An official website posting to the Alphabet Incubator Blockchain (ABC) is a hash code derived from the certificate used as a double security technique.

The final result of data transformation is described as a digital certificate authenticated using the blockchain protocol. The hash code and QR Code are embedded on the digital certificate for convenient access via the official website.

In accordance with the results of the research that has been described, then to reduce the level of forgery of certification of an institution, especially education, blockchain technology as a hexadecimal 64-digit hash code and data security in the form of a QR Code can be implemented. As well as digital certificates generated in research can be said to have immutable, ubiquitous and authenticated values.

3.4. Validation Process

Each certificate that has been embedded in the blockchain is validated in the Verify menu section.

Figure 7. Users have options to upload files in PDF format. The results will be displayed with complete information about the blockchain authentication.

Figure 8. shows the Blockchain Field section that this certificate has been authenticated, with a document hash included. There are two types of document hashes made in this implementation: a unique hash from ABC with the letter ABC code at the beginning of the hash and a unique hash from Vexanium. Vexanium is a public blockchain that works asynchronously to link each certificate to the blockchain.

Figure 9. displays certificates linking the blockchain system. Due to its transparent property, every certificate embedded with a blockchain hash can be authenticated on the ABC official site and subsequently auto verified on the public blockchain <https://explorer.vexanium.com/> by comparing the corresponding Vexanium hash listed in details certificate information.

This implementation can be considered unprecedented novel in the development of blockchain technology. There has not been sufficient research discussion on the authentication and validation of certificates to the extent of our knowledge. Many blockchain types of research focus more on cryptocurrency (Alammary et al., 2019; Franzoni et al., 2019). Thorough dissemination of authenticating certificates embedded in blockchain in the form of digital assets has been layout comprehensively.

No	Email Address	Nama Lengkap	Event	Status	NIM/NIK	Asal Universitas	Hash
1	yudi.sulaeman@raharja.info	Yudi Sulaeman	Liga HA #1	PESERTA	1731498896	Universitas Raharja	ZcGDsqpb3do2N08mAzR-mLicw2N7FwRrmlyFbasMaes=
2	abdullah.dwi@raharja.info	Abdullah Dwi Srenggini	Liga HA #1	PESERTA	2012528903	Universitas Raharja	6KXeBs2QN9W46R2eZt4huMDsDIGRKxSJ2nfQEaR_SOE=
3	marviola@raharja.info	Marviola Hardini	Liga HA #1	PESERTA	1621494208	Universitas Raharja	40mBVDEcF6g9P9Zg0DNHmL09c1B3Zhs6gjJZtd7Jzpg=
4	ikbal.budiono@raharja.info	IKBAL BUDIONO	Liga HA #1	PESERTA	1731499944	Universitas Raharja	ym06WJbTBc3X0n2hHPWC-iSS_xRm9-wKHaipQYxwNSs=

Figure 6. Hash Code on Official Site.

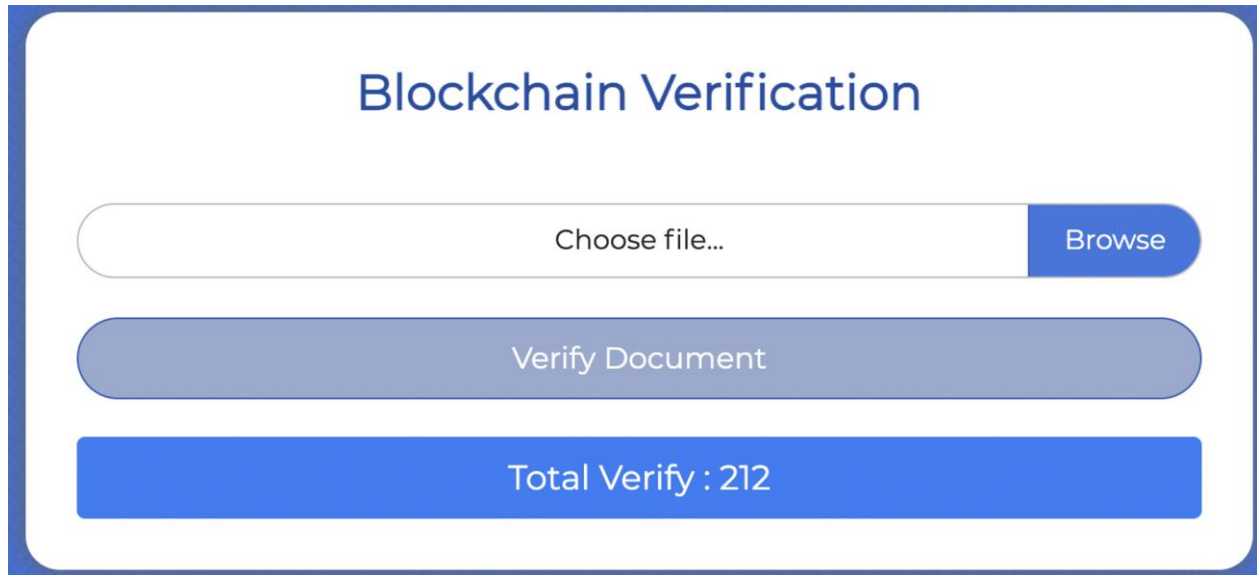


Figure 7. Verify Document.

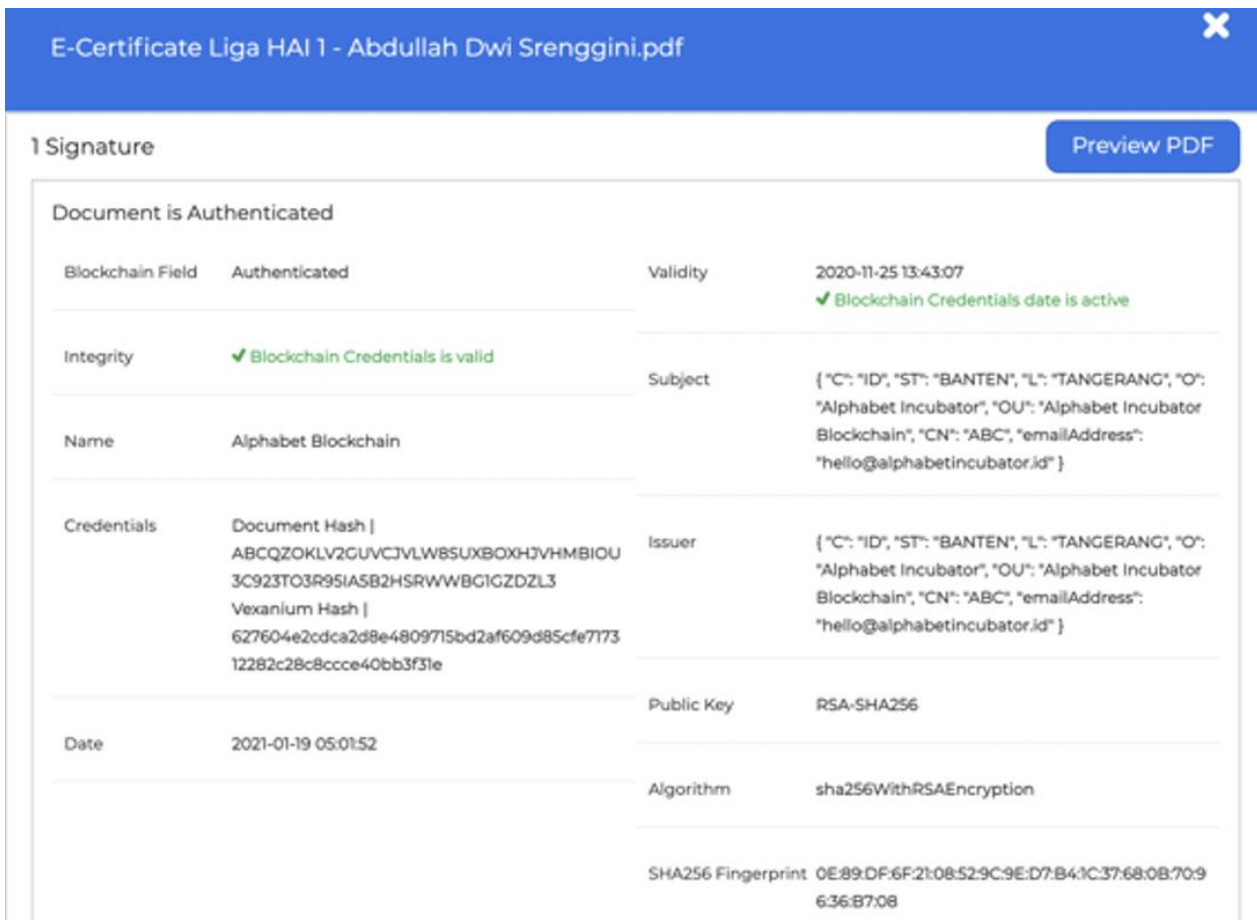


Figure 8. Detail Information Certificate.

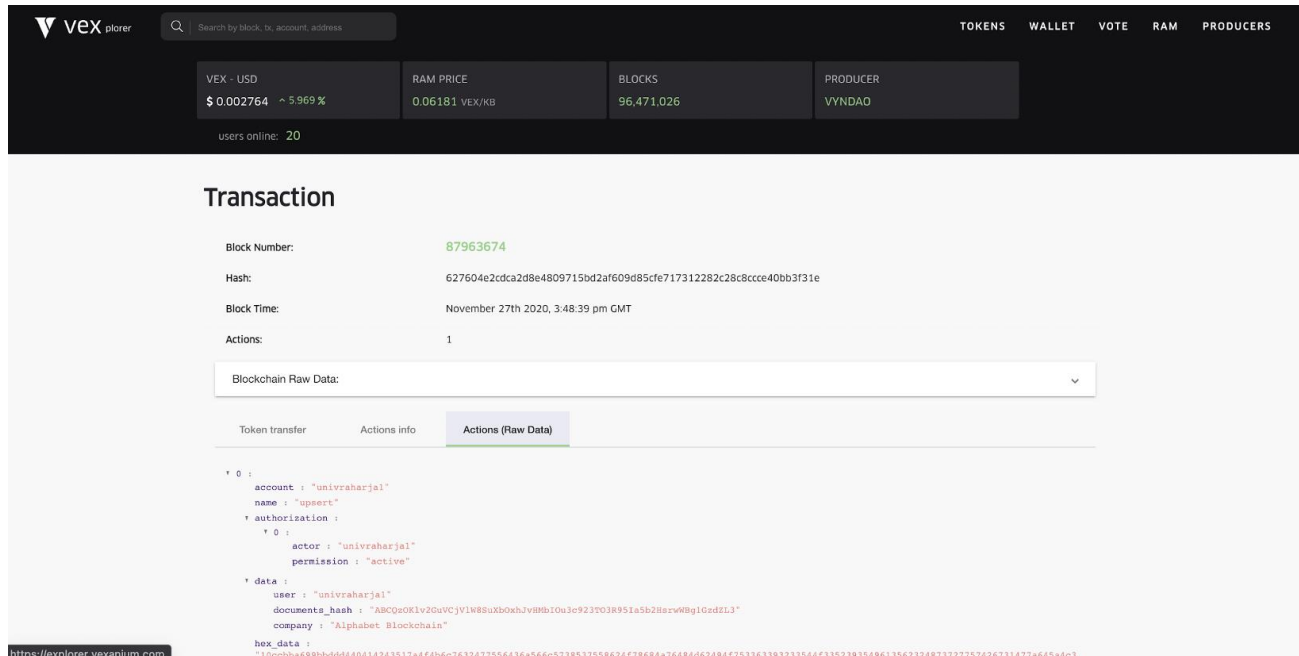


Figure 9. Certificated on Blockchain.

4. Conclusions

Based on the results and discussion that have been outlined, it can get 7 (seven) conclusions in this study, namely:

1. Data security built into the blockchain protocol are some of the most important innovations in the history of computer science and data security education.
2. An education certificate collaborated with blockchain technology ensures data has immutable character.
3. The blockchain technology used in securing educational institution certificate data in this study is SHA-256.
4. Blockchain-based certificates that are created in digital form allow it to be stored for a long period of time.
5. Blockchain can serve various purposes and focus on various aspects, such as security, speed and versatility.
6. Blockchain technology has the potential, not only to align with the development of smart cities, IoT, and circular economy, but in relation to the internet, to form a base layer to enable these technologies to reach their full potential.
7. Six universities have currently participated in a joint consortium to implement this blockchain protocol to digital assets. More universities in other parts of the countries, particularly in remote areas, have agreed to join the consortium soon. If this happens, we can convince more stakeholders to participate in the platform and create a more grand scale holistic scheme of blockchain networks securing digital assets in educational institutions.

Acknowledgments

The author would like to thank Ristek-BRIN, Kominfo Tangerang, University of Raharja, for financial support and for providing a place to support this research through research system analysis. And this research has been funded by a PPD grant number Based on Decree Number 16/E1/KPT/2020.

References

- Adiyanto, A., & Febrianto, R. (2020). Authentication Of Transaction Process In E-marketplace Based On Blockchain technology. *Aptisi Transactions On Technopreneurship (ATT)*, 2(1), 68–74. <https://doi.org/10.34306/att.v2i1.71>
- Aggarwal, S., Chaudhary, R., Aujla, G. S., Kumar, N., Choo, K.-K. R., & Zomaya, A. Y. (2019). Blockchain for smart communities: Applications, challenges and opportunities. *Journal of Network and Computer Applications*, 144, 13–48. <https://doi.org/10.1016/j.jnca.2019.06.018>
- Aini, Q., Hariguna, T., Putra, P. O. H., & Rahardja, U. (2019). Understanding how gamification influences behaviour in education. *International Journal of Advanced Trends in Computer Science and Engineering*, 8(1.5), 269–274. <https://doi.org/10.30534/ijatcse/2019/4781.52019>

- Aini, Q., Rahardja, U., Tangkaw, M. R., Santoso, N. P. L., & Khoirunisa, A. (2020). Embedding a Blockchain Technology Pattern Into the QR Code for an Authentication Certificate. *Jurnal Online Informatika*, 5(2), 239-244.
<https://doi.org/10.15575/join.v5i2.583>
- Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-based applications in education: A systematic review. *Applied Sciences*, 9(12), 2400.
<https://doi.org/10.3390/app9122400>
- Ante, L. (2020). Smart contracts on the blockchain – A bibliometric analysis and review. *Telematics and Informatics*, 101519.
<https://doi.org/10.1016/j.tele.2020.101519>
- Beck, R., & Müller-Bloch, C. (2017). *Blockchain as radical innovation: a framework for engaging with distributed ledgers as incumbent organization*. *Proceedings of the 50th Hawaii International Conference on System Sciences*.
- Bergstra, J. A., & Burgess, M. (2018). *Blockchain Technology and its Applications A Promise Theory view-V0*. 11.
- Brilliantova, V., & Thurner, T. W. (2019). Blockchain and the future of energy. *Technology in Society*, 57, 38–45.
<https://doi.org/10.1016/j.techsoc.2018.11.001>
- Dabbagh, M., Sookhak, M., & Safa, N. S. (2019). The evolution of blockchain: A bibliometric study. *Ieee Access*, 7, 19212–19221.
<https://doi.org/10.1109/ACCESS.2019.2895646>
- Durand, A., Gremaud, P., & Pasquier, J. (2018). Resilient, crowd-sourced LPWAN infrastructure using blockchain. *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 25–29.
<https://doi.org/10.1145/3211933.3211938>
- Ensmenger, N. (2018). The environmental history of computing. *Technology and Culture*, 59(4), S7–S33.
<https://doi.org/10.1353/tech.2018.0148>
- Franzoni, A. L., Cárdenas, C., & Almazan, A. (2019). Using Blockchain to Store Teachers' Certification in Basic Education in Mexico. *2019 IEEE 19th International Conference on Advanced Learning Technologies (ICALT)*, 2161, 217–218.
<https://doi.org/10.1109/ICALT.2019.00070>
- George, R.P., Peterson, B.L., Yaros, O., Beam, D.L., Dibbell, J.M. and Moore, R.C. (2019). Blockchain for business. *Journal of Investment Compliance*, 20(1), 17-21.
<https://doi.org/10.1108/JOIC-01-2019-0001>
- Guritno, S., & Rahardja, U. (2011). *Theory and Application of IT Research: Metodologi Penelitian Teknologi Informasi*. Penerbit Andi.
- Guustaaf, E., Rahardja, U., Aini, Q., Maharani, H. W., & Santoso, N. A. (2020). Blockchain-based Education Project. *Aptisi Transactions on Management (ATM)*, 5(1), 46–61.
<https://doi.org/10.33050/atm.v5i1.1433>
- Hariguna, T., Rahardja, U., Aini, Q., & Nurfaizah. (2019). Effect of social media activities to determinants public participate intention of e-government. *Procedia Computer Science*, 161, 233–241.
<https://doi.org/10.1016/j.procs.2019.11.119>
- Hepp, T., Wortner, P., Schönhals, A., & Gipp, B. (2018). Securing physical assets on the blockchain: Linking a novel object identification concept with distributed ledgers. *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 60–65.
<https://doi.org/10.1145/3211933.3211944>
- Heriyanto, A. P. (2016). *Mobile Phone Forensics: Theory: Mobile Phone Forensics dan Security Series*. Penerbit Andi.
- Ho, S. M., Kao, D., & Wu, W.-Y. (2018). Following the breadcrumbs: Timestamp pattern identification for cloud forensics. *Digital Investigation*, 24, 79–94.
<https://doi.org/10.1016/j.diin.2017.12.001>
- Hu, Y.-C., Lee, T.-T., Chatzopoulos, D., & Hui, P. (2018). Hierarchical interactions between ethereum smart contracts across testnets. *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 7–12.
<https://doi.org/10.1145/3211933.3211935>
- Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, 49, 114–129.
<https://doi.org/10.1016/j.ijinfomgt.2019.02.005>
- Komputer, W. (2013). *The Best Encryption Tools*. Elex Media Komputindo.
- Laurence, T. (2019). *Blockchain for dummies*. John Wiley & Sons.
- Lee, J. Y. (2019). A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. *Business Horizons*, 62(6), 773–784.
<https://doi.org/10.1016/j.bushor.2019.08.003>

- Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain based data integrity service framework for IoT data. *2017 IEEE International Conference on Web Services (ICWS)*, 468–475.
<https://doi.org/10.1109/ICWS.2017.54>
- Lizcano, D., Lara, J. A., White, B., & Aljawarneh, S. (2020). Blockchain-based approach to create a model of trust in open and ubiquitous higher education. *Journal of Computing in Higher Education*, 32(1), 109–134.
<https://doi.org/10.1007/s12528-019-09209-y>
- Ma, Z., Sha, E. H.-M., Zhuge, Q., Jiang, W., Zhang, R., & Gu, S. (2020). Towards the design of efficient hash-based indexing scheme for growing databases on non-volatile memory. *Future Generation Computer Systems*, 105, 1–12.
<https://doi.org/10.1016/j.future.2019.07.035>
- Margulis, A., Boeck, H., & Laroche, M. (2020). Connecting with consumers using ubiquitous technology: A new model to forecast consumer reaction. *Journal of Business Research*, 121, 448–460.
<https://doi.org/10.1016/j.jbusres.2019.04.019>
- Mattila, J. (2016). *The blockchain phenomenon—the disruptive potential of distributed consensus architectures*. ETLA working papers.
- Maulani, G., Rahardja, U., Hardini, M., I'zzaty, R. D., Aini, Q., & Santoso, N. P. L. (2020). Educating Farmers Using Participatory Rural Appraisal Construct. *2020 Fifth International Conference on Informatics and Computing (ICIC)*, 1–8.
<https://doi.org/10.1109/ICIC50835.2020.9288652>
- Mohammed, D., Aisha, N., Himki, A., Dithi, A., & Ardianto, A. Y. (2020). Blockchain Is Top Skill For 2020. *Aptisi Transactions on Technopreneurship (ATT)*, 2(2), 180–185.
<https://doi.org/10.34306/att.v2i2.101>
- Muzayana, A., Karima, A., & Kom, S. (n.d.). *Implementasi Delegated Computation Pada Public Cloud Menggunakan Algoritma Fully Homomorphic Encryption*.
- Nurhaeni, T., Karts, K. W., & Hardini, M. (2019). Viewboard Effectiveness on Raharja Internet Cafe Website as Sales Information Submission Media. *Aptisi Transactions On Technopreneurship (ATT)*, 1(1), 20–26.
<https://doi.org/10.34306/att.v1i1.6>
- Pal, O., Alam, B., Thakur, V., & Singh, S. (2019). Key management for blockchain technology. *ICT Express*. 7(1), 76–80.
<https://doi.org/10.1016/j.icte.2019.08.002>
- Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. *New Economic Windows* (pp. 239–278).
https://doi.org/10.1007/978-3-319-42448-4_13
- Rahardja, I. U., & Raharja, S. (2009). Artificial informatics. *2009 4th IEEE Conference on Industrial Electronics and Applications, ICIEA*, 3064–3067.
<https://doi.org/10.1109/ICIEA.2009.5138764>
- Rahardja, U., Aini, Q., Graha, Y. I., & Khoirunisa, A. (2019). *Implementation of Gamification into Management of Education for Motivating Learners. Proceeding Interuniversity Forum for Strengthening Academic Competency*, 1(1), 209.
- Rahardja, U., Bist, A. S., Hardini, M., Aini, Q., & Harahap, E. P. (2020). *Authentication of Covid-19 Patient Certification with Blockchain Protocol. International Journal of Advanced Science and Technology*, 29(8s), 4015–4024.
- Rahardja, U., Hardini, M., Al Nasir, A. L., & Aini, Q. (2020, November). Taekwondo sports test and training data management using blockchain. In *2020 Fifth International Conference on Informatics and Computing (ICIC)* (pp. 1–6). IEEE.
<https://doi.org/10.1109/ICIC50835.2020.9288598>
- Selimi, M., Kabbinala, A. R., Ali, A., Navarro, L., & Sathiaselalan, A. (2018). Towards blockchain-enabled wireless mesh networks. *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 13–18.
<https://doi.org/10.1145/3211933.3211936>
- Sellami, L., Sellami, K., & Tiako, P. F. (2019). Efficient Management of Security for Supporting Intrusion Detection in Ubiquitous and Pervasive Environments. *Procedia Computer Science*, 155, 402–409.
<https://doi.org/10.1016/j.procs.2019.08.056>
- Sicilia, M.-A., García-Barriocanal, E., Sánchez-Alonso, S., & Cuadrado, J.-J. (2019). Decentralized Persistent Identifiers: a basic model for immutable handlers. *Procedia Computer Science*, 146, 123–130.
<https://doi.org/10.1016/j.procs.2019.01.087>
- Singhal, B., Dhameja, G., & Panda, P. S. (2018). *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*. Apress.
- Skinner, C. (2016). *ValueWeb: How fintech firms are using bitcoin blockchain and mobile technologies to create the Internet of value*. Marshall Cavendish International Asia Pte Ltd.

Sudaryono, Rahardja, U., & Harahap, E. P. (2019). Implementation of Information Planning and Strategies Industrial Technology 4.0 to Improve Business Intelligence Performance on Official Site APTISI. *Journal of Physics: Conference Series*, 1179(1), 0–7.

<https://doi.org/10.1088/1742-6596/1179/1/012111>

Sunarya, P. A., Rahardja, U., Sunarya, L., & Hardini, M. (2020). The Role Of Blockchain As A Security Support For Student Profiles In Technology Education Systems. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, 4(2), 203-207.

Swan, M. (2018). Blockchain enlightenment and smart city cryptopolis. *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 48–53.

<https://doi.org/10.1145/3211933.3211942>

Teece, D. J. (2010). Business models, business strategy and innovation. *Long Range Planning*, 43(2–3), 172–194.

<https://doi.org/10.1016/j.lrp.2009.07.003>

Tenorio-Fornés, A., Hassan, S., & Pavón, J. (2018). Open peer-to-peer systems over blockchain and ipfs: An agent oriented framework. *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 19–24.

<https://doi.org/10.1145/3211933.3211937>

Wei, P., Wang, D., Zhao, Y., Tyagi, S. K. S., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems*, 102, 902–911.

<https://doi.org/10.1016/j.future.2019.09.028>

Whyte, C. (2019). Cryptoterrorism: Assessing the utility of blockchain technologies for terrorist enterprise. *Studies in Conflict & Terrorism*, 1–24.

<https://doi.org/10.1080/1057610X.2018.1531565>

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.

<https://doi.org/10.33050/atm.v2i2.789>

Zainuddin, A., Junaidi, J., & Putra, R. D. (2017). Design of E-Commerce Payment System at Tokopedia Online Shopping Site. *Aptisi Transactions On Management*, 1(2), 143–155.

<https://doi.org/10.33050/atm.v1i2.666>

Zeng, Q., Zhang, X., Wang, T., Shi, P., Fu, X., & Feng, C. (2019). BBCPS: A Blockchain Based Open Source Contribution Protection System. *International Conference on Blockchain and Trustworthy Systems*, 662–675.

https://doi.org/10.1007/978-981-15-2777-7_54