Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 17 No. 18 (2023) | OPEN ACCESS

https://doi.org/10.3991/ijim.v17i18.41823

PAPER

A Blockchain-Secure Mobility Data in Smart Campus

Fachrul Kurniawan[1](✉), Dian Permana Putra[1], Jehad Hammad[2], Anton Satria Prabuwono[3]

[1]Department of Informatic Engineering, Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia

[2]Al Quds Open University of Palestine, Abu Dis, Palestine

[3]King AbdulAziz University, Jeddah, Saudi Arabia

fachrulk@ti.uin-malang.ac.id

ABSTRACT

Acquiring knowledge of the patterns of human mobility within a university setting is a critical endeavor that can facilitate the development of effective strategies for future work programs. It is essential to ascertain the positions of campus inhabitants as they engage in daily activities that align with the institution's work plan framework. Nonetheless, the paramount challenge associated with the presence of personal data on human movement is ensuring the utmost security of this sensitive information. Blockchain technology offers a solution by enabling the safeguarding of personal data through the decentralization of information, wherein individuals act as controllers in a distributed cloud network. In the present study, a straightforward system comprising GPS sensors and a Raspberry Pi is employed to detect personnel's location data. The SHA256 algorithm is utilized to generate a hash that connects the constituent blocks, thereby significantly enhancing data security. The intricate hash computation is validated through the implementation of proof-of-work, which generates pertinent binary data at an expeditious block mining time of 16.64 milliseconds. This approach effectively thwarts cyberattacks and ensures the maximum protection of data.

KEYWORDS

blockchain technology, smart campus, secure data, SHA-256

1 INTRODUCTION

Campus development has increasingly become a pressing concern as urban centers worldwide embrace the principles of smart city-based growth. Given the escalating population and the complexities of regional challenges that emerge, the educational sector is poised to serve as the primary driving force for resolution, acting as a shared point of reference. This is consistent with the issue of dwindling natural resources, which necessitates a profound understanding from every global inhabitant, with higher education being a potential solution.

The rapid advancement of online information technology has significantly altered human behavior as well as the human resources that underpin openness and transparency. The integration of technology has gradually and inevitably instigated fundamental transformations in interactions with campus services, characterized

Kurniawan, F., Putra, D.P., Hammad, J., Prabuwono, A.S. (2023). A Blockchain-Secure Mobility Data in Smart Campus. *International Journal of Interactive Mobile Technologies (iJIM)*, 17(18), pp. 55–66. https://doi.org/10.3991/ijim.v17i18.41823

Article submitted 2023-06-23. Revision uploaded 2023-07-18. Final acceptance 2023-07-17.

by the absence of face-to-face meetings and reduced time requirements [1–3]. Expedited service must be an essential component of smart Islamic campus development. All campus members should undoubtedly adopt openness and transparency as critical parameters in the implementation of information technology systems [4] [5]. Consequently, universities must anticipate and adapt to these changes in bureaucratic systems, actively involving all campus members in the development and execution of programs in alignment with their respective fields and objectives [1–5].

The smart campus paradigm encompasses a direct and transactional relationship between students, faculty members, and institution-affiliated staff. This concept is predicated on services that universities, as academic hubs, are obliged to provide [5–7]. The adoption of a smart campus-based approach galvanizes every stakeholder to actively contribute to the evolution of a global campus. Feasible roles include offering feedback on service quality, facilitating academic life, and maintaining a healthy campus environment that upholds scholarly ethics. Sustainability is paramount to smart campus-based development, as success hinges on consistency and commitment to growth initiatives.

A smart campus fosters an inclusive environment, enabling all campus members to actively participate in services provided by the institution to students and the wider community in line with their primary responsibilities and functions [5]. This facilitates the development of hardware infrastructure, application systems, and, ultimately, the success of policies that support smart campus-based initiatives.

However, it is important to situate this study within the existing literature on smart campus development and implementing blockchain technology in the educational sector. Several studies have explored the concept of smart campuses and technology integration in higher education institutions. For example, Pandita and Kiran [8] investigated the impact of technology integration on student engagement and learning outcomes in a smart campus environment. Their findings highlighted the positive effects of technology integration on student satisfaction and academic performance.

Regarding blockchain technology, previous research has demonstrated its potential in various domains, including education. Bucea-Manea-Țoniş et al. [9] studied blockchain applications for secure credentialing in higher education. Their findings indicated that blockchain-based systems could enhance academic credentials' security, privacy, and integrity.

Furthermore, in communication and data security, blockchain technology has been explored in healthcare and supply chain management. For instance, Chelladurai and Pandian [10] proposed a blockchain-based system for secure and transparent medical data sharing among healthcare providers. Their study highlighted the potential of blockchain for improving data privacy and interoperability in the healthcare sector.

The primary necessity for communication within an intelligent academic campus is the safeguarding of data. Blockchain technology presents a promising solution, warranting further exploration and proposition. The central issue to address is the implementation of a security system based on blockchain technology for communication at an Islamic state university, with the ultimate goal of actualizing a sophisticated Islamic academic environment [11]. Building on the existing literature, this paper aims to evaluate the block-mining time of the Proof of Work process for hash value validation, employing the SHA-256 algorithm. Blockchain technology affords a decentralized and trustworthy consensus, enabling the storage and access of medical product data throughout the logistics process for both parties because it is secured by smart contracts.

2 METHODS

Figure 1 presents the research workflow employed to develop a simulation pertaining to the data security of campus mobility, particularly focusing on the activities of campus resources, such as faculty, students, and staff. This process involves collecting GPS location information for all mobility between buildings within the campus, followed by the implementation of the SHA-256 algorithm and proof of work (PoW) to process the data.

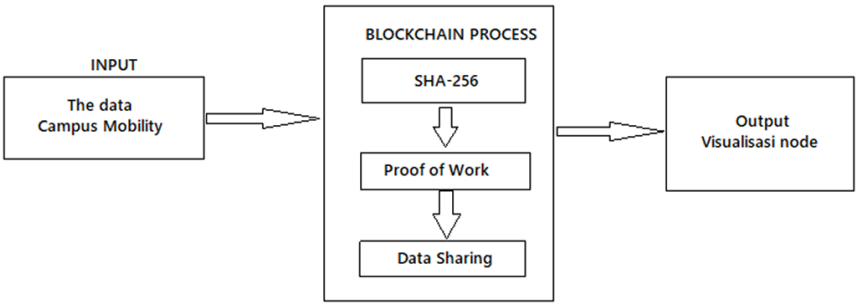

Fig. 1. Secure mobility data campus research flow

By following this methodology, we can ensure the secure and decentralized storage of mobility data within the smart campus environment, leveraging blockchain technology and cryptographic algorithms to enhance data security and integrity.

3 MAIN CONTRIBUTION

In this scholarly article, we aim at offering a significant contribution to the field of data communication security systems, particularly those implemented on university campuses, by employing the Secure Hash Algorithm 256 (SHA-256) [12] [13]. We propose utilizing blockchain technology as a decentralized database to store information pertaining to students, faculty members, and all university assets, encompassing the administrative hierarchy from the rectorate to individual academic programs. This distributed storage model is built on both the server and the nodes within the blockchain network. To ensure comprehensive monitoring of data modifications within the smart campus application, blockchain technology can be directly applied. The incorporation of cryptographic techniques helps to bolster data security, rendering it less susceptible to compromise. The SHA-256 algorithm operates by taking inputs and generating a distinct 256-bit hash output [9]. Within the blockchain nodes, each block possesses a hash derived from the data it contains. The hash of the preceding block is also employed as an input for calculating the current block's hash, thereby establishing a consistent and tamper-resistant blockchain [14] [15].

4 SMART CAMPUS CONCEPT

The concept of a smart campus model emphasizes a resident-centric approach that leverages information technology to develop systems and environments at the forefront of implementation. This model aims to provide comprehensive services to campus residents, ultimately fulfilling the university's vision and mission to become

a preeminent institution with global recognition. By fostering focused and purposeful interactions, the smart campus model facilitates constructive and holistic development, thereby inspiring campus residents to actively engage in and contribute to the achievement of goals set forth by university leadership.

The features are comprehensively incorporated into a unified service system, housed within a single network framework situated in the data center that employs big data technology. By adopting this paradigm, it is anticipated that all campus operations will be subject to continuous observation and supervision, thereby enhancing overall management. Furthermore, service facilities encompassing education and instruction, research, and community engagement will be increasingly integrated and balanced in their execution. As stakeholders, campus community members can access all services and contribute their input through mobile-based platforms, desktop computers, or internet-enabled devices such as notebooks, tablets, or smartphones.

5 BLOCKCHAIN

Each transaction within the blockchain must be meticulously documented, disseminated, and rendered transparent. During these exchanges, digital assets, encompassing currency or other valuable resources, are transferred. Every node within the blockchain network bears the responsibility of validating transactions and maintaining a replica of the data. Nodes may manifest as computer processes or hardware operating on the network. To guarantee data security and authentication, blockchain systems employ cryptographic algorithms [16] [17]. Such encryption safeguards the data in transit and precludes the possibility of compromise [18]. The block consensus protocol serves to regulate and administer transactions, ensuring that all nodes within the network reference an identical data version [16] [19]. Smart contracts, which are computer codes stored on the blockchain, facilitate the automation of business operations. These contracts ascertain that all executed transactions adhere to the predefined stipulations. The blockchain embraces the notion of an immutable ledger, signifying that once a transaction is incorporated into the network, it cannot be altered or expunged [20]. This engenders a sense of security and trust among blockchain users.

6 SHA-256 ALGORITHM

The SHA256 algorithm is employed to compute the message digest value for messages with a maximum length of 264 bits. This algorithm necessitates a message schedule comprising 64 elements of 32-bit words, eight 32-bit variables, and a storage variable for eight 32-bit hash values [13]. The outcome of the SHA256 algorithm is a 256-bit message digest. As delineated in the SHA256 reference, the input message is transformed into a 256-bit message digest format. In accordance with secure hash signatures, standard input messages with lengths shorter than 264 bits are processed in 512-bit units and result in a 256-bit message summary [21].

7 PROOF OF WORK

Proof of Work (PoW), employed in Bitcoin, is utilized to secure the blockchain ledger from undesirable alterations. PoW in Bitcoin operates as follows: all information regarding the values contained within a candidate block is computed based on its hash value. The generated hash value must adhere to stringent criteria established by the system. If the hash value does not meet these requirements, then the blockchain

calculation is repeated by modifying the nonce value. The nonce is a value that lacks inherent meaning but is intended to be added to the block in order to generate a hash value that complies with the specified conditions [22]. If the hash value does not satisfy the conditional value, the nonce value is replaced until the miner obtains a hash value that meets the requirements. The validation measure using Proof of Work (PoW) validates the hash value present in each block, employing the following equation (1).

$$H\,(N \,||\, Prev\_hash \,||\, Tx \,||\, Tx \,||\, \ldots\, Tx) < Target). \tag{1}$$

According to equation (1), (N) represents the nonce of the block, (*Prev_hash*) denotes the hash value of the previous block, (*Tx*) signifies the mobility data contained within the block, and (*Target*) corresponds to the predetermined target value (network difficulty). In the aforementioned Proof of Work concept, the hash value of a block must be less than the established target value. Once the hash value of each block reaches the predetermined target, the hash value of that block is successfully validated [23].

8 RESULT AND DISCUSSION

In this article, campus mobility is conceptualized as the relocation of campus resources due to the presence of devices that must be attached and transported wherever they go, along with their respective vehicles. The proposed approach comprises three primary components:

(a) the acquisition of location displacement data,
(b) the transmission of mobility data, and
(c) the security of mobility data.

The input data utilized consists of mobility data of resources in motion, functioning as nodes within the blockchain network. Prior to data collection, campus resources must first undergo a registration process as new nodes within the blockchain network. The mobility data encompasses the index, previous hash, timestamp, latitude and longitude coordinates, hash, and nonce. The following presents some test results of the SHA-256 algorithm, which were obtained by sampling campus community mobility data from building A (the record office) to building B (the library) and building C (the science and technology center) in November 2022;

Date: 2022/01/11
timestamp: 1641907429.811641907429
Time: 20:23:49
bin: 0
indeks nol: 0
nonce: 1
diff: 1
hash: 93e8e90bd35edc976f2bd54ac5c41c0acc5686cb873190580cac4eaa9c81c543
prevHash: 21774764ec334c921a4b2eb62a60785e3370fc881283a83ec359836461d3eff9
fullbin:
0b10010011111010001110100100001011110100110101111011011100100101110110111100101011110101010100101011000101110001000001110000001010110011000101011010000110110010111000011100110001100100000101100000000110010101100010011101010101010011100100000011100010101000011

hash: 2df6e1bf3dc703b497165c133558d118bdae3158bd2fa
8099aae4664670d767d
prevHash:93e8e90bd35edc976f2bd54ac5c41c0acc5686cb873190580cac4eaa9c81c543
fullbin:
0b10110111110110111000011011111100111101110001110000001110110100100
10111000101
10010111000001001100110101010110001101000100011000101111011010111000
1100010101
10001011110100101111101010000000100110011010101011100100011001100
0110011100
001101011011001111101
bin: 0
indeks nol: 0
nonce: 8
diff: 1
timestamp: 1641907429.91 – 1641907429
date: 2022/01/11
time: 20:23:49data: 16419074292022/01/1120:23:49-
7.95077064936154112.6078831775801293e8e90bd35edc976f2bd54ac5c41c0acc5686cb873190
580cac4eaa9c81c54381

Then the second test was carried out with the appropriate results, and the following is the second sample test data.

Date: 2022/01/11
Time: 20:23:50
hash: 8889930a515a78468a785240f8c42477673c04d9b509a4007969d22ff6e064b9
prevHash:bd81befa6664d5d2fa922491d2080db1ca4575725806cbd917595d5d3062f3af
fullbin:
0b10001000100010011001001100001010010100010101101001111000010001101
00010100111
10000101001001000000111110001100010000100100011101110110011100111
000000010011
01100110110101000010011010010000000000011110010110100111010010001
111111110110
11100000011001001011100 1
bin: 0
indeks nol: 0
nonce: 6
diff: 1
timestamp: 1641907430.28
1641907430
data: 16419074302022/01/1120:23:50-
7.949995839448067112.60665735084142bd81befa6664d5d2fa922491d2080db1ca45
75725806c
bd917595d5d3062f3af61

hash: 168d5a83f09ee82a992e5f1658a3cdb385c089070bd9f7587862074b430885a8
prevHash:8889930a515a78468a785240f8c42477673c04d9b509a4007969d22ff6e064b9

fullbin:
0b1011010001101010110101000001111110000100111101110100000101010100
110010010111
0010111110001011001011000101000111100110110110011100001011100000001
000100100000
1110000101111011001111101110101100001111000011000100000011101001010
101000011000
0100010000101101010000bin: 0
indeks nol: 0
nonce: 1
diff: 1
timestamp: 1641907430.37
1641907430
date: 2022/01/11
time: 20:23:50
data: 16419074302022/01/1120:23:50-
7.948409930300205112.606349860336088889930a515a78468a785240f8c424776
73c04d9b509a
4007969d22ff6e064b911

In accordance with the sampled implementation, the two tests demonstrate that the hash and previous hash values are congruent, signifying that the SHA256 hashing method functions effectively for encryption processes and maintains interconnectivity among blocks [2] [3]. The validity of these values can be observed from the results of the trial conducted on each block, as the data from every resource undergoes mobility. We will include the data from 20 test samples employing the SHA-256 algorithm at the end of this paper. When represented graphically, as in Figure 2, it is evident that the rate of invalidity is remarkably minimal.

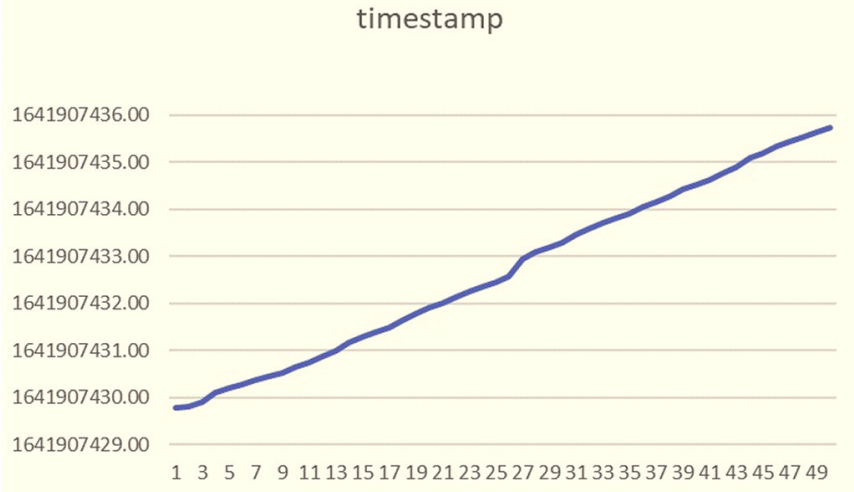

Fig. 2. Matching accuracy rate using SHA-256

The efficacy of proof of work is evident in its current implementation. This is demonstrated by the presence of a zero following the initial numeral, signifying a binary value that adheres to the predetermined target difficulty [22] [24]. Within a sample of 20 binary data points derived from hashing processes, one data point

was generated with block-mining times of 10, 12, 50, and 108 milliseconds; two data points exhibited block-mining times of 80 milliseconds; five data points displayed block-mining times of 60 milliseconds; six data points had block-mining times of 70 milliseconds; and three data points presented block-mining times of 90 milliseconds. The average block-mining time was determined to be 16.64 milliseconds. Upon attaining the established target, each block's hash value is deemed successfully validated, and the block-mining time's velocity is ascertained. The initial timestamp value for the proof of work assessment was 1641907429.78.

The subsequent phase involves assessing the security level against forced alterations enacted on mobility data. This trial aims to examine the extent to which the hash value may change. The evaluation was conducted on block ID 38, which indicated a timestamp of 09:53:04, representing the original value that signifies no modifications have occurred. Subsequently, the timestamp was altered to 10:53:04, and the findings revealed that blockchain technology operates in accordance with the theoretical premise that prohibits changes, denoting that the attempted alterations were unsuccessful, as demonstrated in Figure 3.

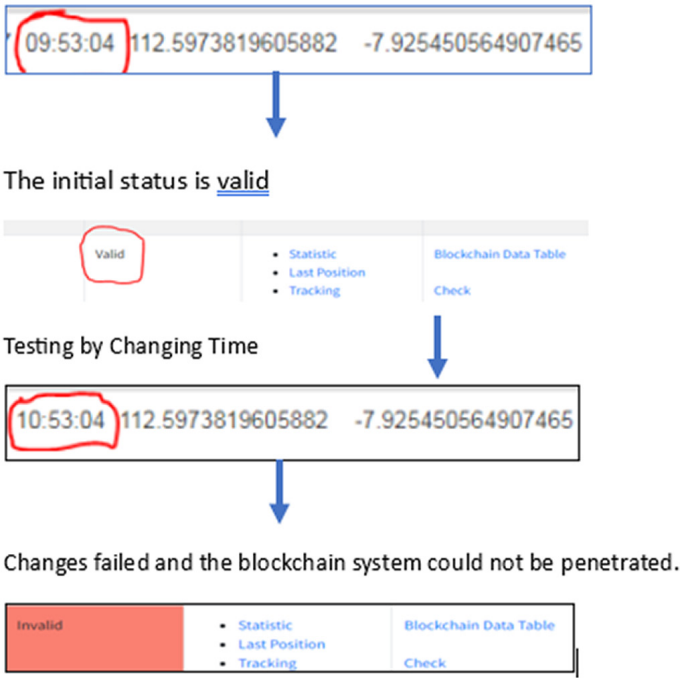

Fig. 3. Hacking testing on the mobility data blockchain system

The proposed implementation of the SHA-256 algorithm for securing mobility data within the blockchain network of a smart Islamic campus yielded promising results. However, it is important to discuss these findings in the context of other similar studies to highlight the novelty and contribution of this research. In the realm of data security and integrity, traditional cryptographic methods have been widely utilized. However, the centralized nature of these methods introduces vulnerabilities and reliance on trusted authorities for verification. Blockchain technology offers a decentralized and transparent alternative for data security. When comparing the obtained results with existing methods, it is essential to consider other blockchain-based security approaches, which can be seen in Table 1.

Table 1. Comparison with the existing method

Study	Method	Block Mining Time (ms)	Key Findings	Contribution
[25]	Keccak (SHA-3)	18.89	Implementing SHA-3 on Xilinx FPGAs for IoT applications	The secure hashing process can be accelerated, ensuring the integrity and authenticity of IoT data
[26]	Blake-2	18.90	BLAKE2 provides a high level of security and data integrity, comparable to or surpassing that of MD5	The advantages of using BLAKE2 as a simpler, smaller, and faster alternative to MD5
[27]	Ethash	21.00	The system can enhance security and trust within the embedded environment	Implementing these algorithms on embedded architecture ensures that the blockchain network remains secure and resistant to various attacks
Proposed Study	SHA-256	16.64	Successful implementation of SHA-256 for securing mobility data	Novel application in a smart Islamic campus, emphasis on data security

Table 1 compares the proposed study with existing methods regarding block mining time, key findings, and contribution. The proposed study focuses on implementing the SHA-256 algorithm for securing mobility data on a smart Islamic campus. It emphasizes the successful implementation of SHA-256 and highlights the novel application in the context of a smart campus, with a specific focus on data security. The other studies [25], [26], and [27] utilize different algorithms such as Keccak (SHA-3), Blake-2, and Ethash for various applications. These studies emphasize topics such as implementing SHA-3 on FPGAs for IoT applications, highlighting the advantages of Blake-2 as an alternative to MD5, and enhancing security and trust within the embedded environment. SHA-256 has the fastest block mining time among other methods, as shown in Figure 4. Overall, the proposed study contributes to the field by showcasing the successful implementation of SHA-256 in securing mobility data within a smart Islamic campus, addressing specific requirements, and emphasizing data security in that context.

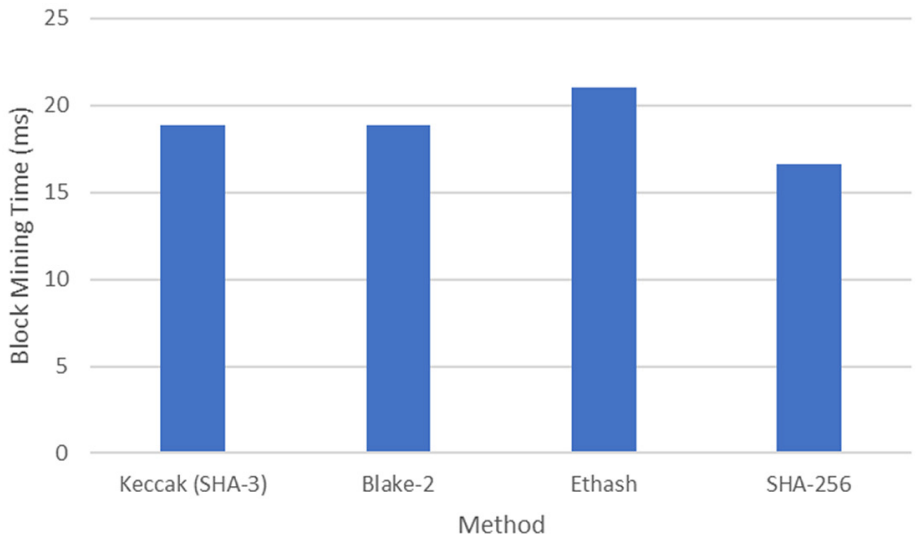

Fig. 4. Comparison with the existing method based on block mining time

While this study successfully implemented the SHA-256 algorithm for securing mobility data within a blockchain network, there are some limitations to consider. Firstly, the research relied on a simulated environment and a limited sample size of mobility data from a specific timeframe. Future work should involve real-world implementation and a larger dataset to validate the effectiveness of the proposed blockchain-based security system in diverse scenarios and over an extended period. Secondly, the study concentrated on the SHA-256 algorithm. Furthermore, future investigations could consider the performance and security implications of other hashing algorithms or explore hybrid approaches that combine different encryption methods within the blockchain system. By recognizing these limitations and proposing future avenues for exploration, researchers can build upon the current study and contribute to advancing blockchain technology in smart campus environments.

9 CONCLUSION

One of the most prevalent hashing algorithms currently employed in blockchain technology is SHA-256. Irrespective of the data provided as input, this algorithm possesses the ability to generate a unique and completely distinct hash. This is of paramount importance, as the foundation of blockchain technology lies in the concept of hashes, which facilitate the verification and authentication of transactions and blocks appended to the network. Moreover, due to the elevated complexity of the SHA-256 algorithm, it is considerably challenging to discover a suitable hash for modifying transaction data or blocks already incorporated into the blockchain. Consequently, the SHA-256 algorithm offers exceptional security, ensuring network resilience and protection when applied to blockchain technology. This underscores the indispensability of the SHA-256 algorithm for blockchain. In addition, it demonstrates the effectiveness of SHA-256 hashing in blockchain technology systems that have been validated. Blocks are sequentially connected through hash values and the preceding hash of each block.

The mining time of blocks in the integrated system is accelerated through the expeditious calculation of the PoW. Empirical evidence from conducted tests indicates that PoW operates efficiently and rapidly, as demonstrated by the number of zeros following the initial 1 in the binary value of each data piece that meets the target difficulty value, with an average mining time of 66.4 milliseconds. Each block generated by the hashing process necessitates the presence of PoW to verify the hash value [19] [22] [24]. As part of the validation procedure, the hash value of each block will be authenticated using PoW. When the hash value of each block converges toward an acceptable level, the block's hash value is deemed successfully validated.

10 ACKNOWLEDGMENT

This research is supported by Universitas Islam Negeri Maulana Malik Ibrahim Malang.

11 CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

12 REFERENCES

[1] Artyom Kosmarski, "Blockchain adoption in academia: Promises and challenges," *Journal of Open Innovation Technology Market and Complexity*, vol. 6, no. 4, p. 117, 2020.

[2] L. Ismail, H. Hameed, M. AlShamsi, M. AlHammadi, N. AlDhanhani, "Towards a blockchain deployment at UAE university: Performance evaluation and blockchain taxonomy," In *ICBCT 2019: Proceedings of the 2019 International Conference on Blockchain Technology*, pp. 30–38, 2019. https://doi.org/10.1145/3320154.3320156

[3] P. Rivera Vargas, C. Lindín Soriano, P. Rivera Vargas, U. Andrés Bello, and C. Carles Lindín Soriano, "Blockchain in the university: A digital technology to design, implement and manage global learning itineraries," *dialnet.unirioja.es*, (Accessed: Apr. 22, 2023).

[4] R. Raimundo et al., "Blockchain system in the higher education," *Eur. J. Investig. Health Psychol. Educ.*, vol. 11, pp. 276–293, 2021. https://doi.org/10.3390/ejihpe11010021

[5] M. Jirgensons, "Blockchain and the future of digital learning credential assessment and management," *Journal of Teacher Education for Sustainability*, vol. 20, no. 1, pp. 145–156, 2018. https://doi.org/10.2478/jtes-2018-0009

[6] Skiba, Editor, and J. Diane, "The potential of blockchain in education and health care," *Nursing Education Perspectives*, vol. 38, no. 4, pp. 220–221, 2017. https://doi.org/ 10.1097/01.NEP.0000000000000190

[7] W. Villegas-Ch, X. Palacios-Pacheco, and M. Román-Cañizares, "Integration of IoT and blockchain to in the processes of a university campus," *Sustainability*, vol. 12, no. 12, p. 4970, 2020. https://doi.org/10.3390/su12124970

[8] A. Pandita and R. Kiran, "The technology interface and student engagement are significant stimuli in sustainable student satisfaction," *Sustainability*, vol. 15, no. 10, p. 7923, 2023. https://doi.org/10.3390/su15107923

[9] R. Bucea-Manea-Ţoniş et al., "Blockchain technology enhances sustainable higher education," *Sustainability*, vol. 13, no. 22, p. 12347, 2021. https://doi.org/10.3390/su132212347

[10] U. Chelladurai and S. Pandian, "A novel blockchain based electronic health record automation system for healthcare," *J. Ambient Intell. Humaniz. Comput.*, vol. 13, no. 1, pp. 693–703, 2022. https://doi.org/10.1007/s12652-021-03163-3

[11] S. Blake-Wilson, D. Johnson, Alfred Menezes, "Key agreement protocols and their security analysis," In *Crytography and Coding. Lecture Notes in Computer Science*, Darnell, M. (Eds.), vol. 1355, Springer, Berlin, Heidelberg, 1997. https://doi.org/10.1007/BFb0024447

[12] R. V. Mankar and S. I. Nipanikar, "C implementation of SHA-256 algorithm," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 6, pp. 167–170, 2013.

[13] A. Sebastian, "Implementasi dan perbandingan performa algoritma hash SHA-1, SHA-256, dan SHA-512," *Skripsi,* Inst. Teknol. Bandung, Bandung, Indonesia, 2007.

[14] I. Chung and Y. Bae, "The design of an efficient load balancing algorithm employing block design," *J Appl Math Comput*, vol. 14, no. 1–2, pp. 343–351, 2004. https://doi.org/10.1007/BF02936119

[15] O. Lee, S. Yoo, and B. Park, "The design and analysis of an efficient load balancing algorithm employing the symmetric balanced incomplete block design," *Information Sciences*, vol. 176, no. 15, pp. 2148–2160, 2006. https://doi.org/10.1016/j.ins.2005.09.004

[16] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Čapkun, "On the security and performance of Proof of Work blockchains," In *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 3–16, 2016. https://doi.org/10.1145/2976749.2978341

[17] A. Aziz, M. T. Riaz, M. S. Jahan, and K. Ayub, "Meta-model for Stress Testing on Blockchain Nodes," In *3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pp. 1–4, 2020. https://doi.org/10.1109/iCoMET48670.2020.9073924

[18] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *Lecture Notes in Computer Science*, vol. 2139, pp. 213–229, 2001. https://doi.org/10.1007/3-540-44647-8_13

[19] I. Gemeliarana and R. F. Sari, "Evaluation of proof of work (POW) blockchains security network on selfish mining," *International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, Yogyakarta, Indonesia, pp. 126–130, 2018. https://doi.org/10.1109/ISRITI.2018.8864381

[20] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," In *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 79–88, 2006. https://doi.org/10.1145/1180405.1180417

[21] A. Kiayias and D. Zindros, "Proof-of-Work sidechains," *Lecture Notes in Computer Science*, vol. 11599, pp. 21–34, 2020. https://doi.org/10.1007/978-3-030-43725-1_3

[22] Z. H. Chin, T. T. V. Yap, and I. K. T. Tan, "On the trade-offs of Proof-of-Work algorithms in blockchains," *Lecture Notes in Electrical Engineering*, vol. 603, pp. 575–584, 2020. https://doi.org/10.1007/978-981-15-0058-9_55

[23] "Blockchain Demo – A visual demo of blockchain technology," https://blockchaindemo.io/ (Accessed: Apr. 22, 2023).

[24] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Čapkun, "On the security and performance of Proof of Work blockchains," In *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 3–16, 2016. https://doi.org/10.1145/2976749.2978341

[25] M. Rao, T. Newe, and I. Grout, "Secure hash algorithm-3 (SHA-3) implementation on xilinx FPGAs, suitable for IoT applications," *Int. J. Smart Sens. Intell. Syst.*, vol. 7, no. 5, pp. 1–6, 2014. https://doi.org/10.21307/ijssis-2019-018

[26] J. P. Aumasson, S. Neves, Z. Wilcox-O'Hearn, and C. Winnerlein, "BLAKE2: Simpler, smaller, fast as MD5," *Lect. Notes Comput. Sci.*, vol. 7954, pp. 119–135, 2013. https://doi.org/10.1007/978-3-642-38980-1_8

[27] T. Frikha, F. Chaabane, N. Aouinti, O. Cheikhrouhou, N. Ben Amor, and A. Kerrouche, "Implementation of blockchain consensus algorithm on embedded architecture," *Secur. Commun. Networks*, vol. 2021, pp. 1–11, 2021. https://doi.org/10.1155/2021/9918697

13 AUTHORS

Fachrul Kurniawan, Department of Informatic Engineering, Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia.

Dian Permana Putra, Department of Informatic Engineering, Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia.

Jehad Hammad, Al Quds Open University of Palestine, Abu Dis, Palestine.

Anton Satria Prabuwono, King AbdulAziz University Jeddah, Saudi Arabia.