The adoption factors of two-factors authentication in blockchain technology for banking and financial institutions

Amir Aizzat Basori[1], Nor Hapiza Mohd Ariffin[2]
[1]Affin Bank Berhad, Kuala Lumpur, Malaysia
[2]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Shah Alam, Malaysia

Article Info

Article history:

Received Sep 29, 2021
Revised Apr 15, 2022
Accepted Apr 22, 2022

Keywords:

Banking and financial institution
Blockchain authentication technology
Risk management
Two-factor authentication

ABSTRACT

Malaysian banks and financial organisations urgently require a secure authentication mechanism. However, there is a lack of research on the factors that drive blockchain authentication technology adoption, notably in Malaysian banks. This study identified the factors impacting adopting blockchain authentication technology in Malaysia. This document will be a roadmap for replacing existing technology utilizing the traditional transaction authorization code (TAC) via a short messaging service (SMS). In addition, this study looks into the elements that influence the new blockchain authentication technology's acceptability in Malaysia. The data was gathered from articles and research papers written by other scholars on blockchain authentication. To examine and categorise the aspects that influence the acceptance of blockchain authentication technology, we used risk management in technology (RMiT) standards to map them. Based on the result, security risk, regulatory support, technology latency, and technology complexity have been established as components of blockchain authentication adoption factors that can be a guideline to implement blockchain authentication in banking and financial institutions in Malaysia. In addition, the findings can contribute as a reference for future researchers to develop models or guidelines for blockchain authentication methods in banking and financial institutions.

Corresponding Author:

Nor Hapiza Mohd Ariffin
Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA
Shah Alam, 40450, Selangor, Malaysia
Email: hapiza@uitm.edu.my

1. INTRODUCTION

Secured authentication is one of the most important success elements for online banking and transactions, and it has become something of a leap of faith for many people [1]. In part, this is because banking and financial institutions (FI) themselves place a high value on trust as the foundation of their customer relationships [2]. Through this principle, banking and FI has evolved from conventional banking, where the customer requires to be physically at the branch to perform identification verification, to mobile banking, where you can perform any transactions anywhere securely [3].

In banking and FI in Malaysia context, two-factor authentication (2FA) was introduced to strengthen the verification mechanism by having a combination of two types of evidence or factors which is knowledge (something only the user know), possession (something only the user has) or inherence (something only the user is) [4]. In today's situation, internet banking uses 2FA, a 10-digit password and short messaging service via transaction authentication code (SMS TAC) number. SMS TAC number is a random 6-digit number sent via SMS to the registered phone number [5]. However, while this has been the factor for many years, hackers and fraudsters still find a way to intercept the security measures by acquiring user passwords and manipulating phone numbers.

Blockchain technology is considered an emerging technology. Blockchain authentication technology adoption studies for authentication method options for banking and FI have never been done before. The problem with adopting blockchain technology is that 40% of the organizations feel that lack of knowledge and understanding of blockchain technology. Another 40% of people think that their organization feels blockchains technology is still a new and emerging technology. While another 37% of organizations think they lack expertise and skills in blockchain technology. There are also no proper guidelines for banking and financial to adopt blockchain authentication technology, specifically in Malaysia [6].

In order to solve the problem mentioned, the study will identify the adoption factors in 2FA blockchain technology implementation based on articles and research done by the past researcher. The adoption factors will prove that blockchain authentication technology as 2FA will be a better option with better security and reliability [7]. Thus, the adoption factors will be analyzed to fit the needs of banking and FI in Malaysia. Furthermore, guideline documentation from Bank Negara Malaysia, risk management in technology (RMiT), will be studied to ensure all adoption factors meet the requirements of banking and FI in Malaysia [8]. The research concludes with a deep understanding of each adoption factor contributing to future research to develop models and guidelines.

2. LITERATURE REVIEW

The literature review on the application of blockchain technology in banking and FI is still far from complete. This was proven by the lack of publication related to blockchain technology adoption. Refer to Figure 1, for a year-wise analysis of the selected literature per type of publication for blockchain technology. It shows that the publication of related blockchain technology has increased significantly over the years. This upward trend highlights blockchain technology's emerging and growing nature and academic interest [9]. A total of 260 research items have been analyzed, and found that 11 domains of blockchain-based applications have been identified. Business-oriented applications represent a large portion with 58 out of the 260 research items, followed by governance, internet of things (IoT), and data management applications. The health-oriented application also received much attention from the scientific community during the last couple of years. For banking and financial institutions, 17 out of 260 items. It shows that blockchain technology in banking and FI is at its early stages, and the research community has yet to produce substantial financial-oriented applications [9]. In order to understand blockchain technology acceptance in banking and FI, research on literature related to blockchain technology adoption is conducted. Table 1 shows publications related to blockchain authentication technology and its description.

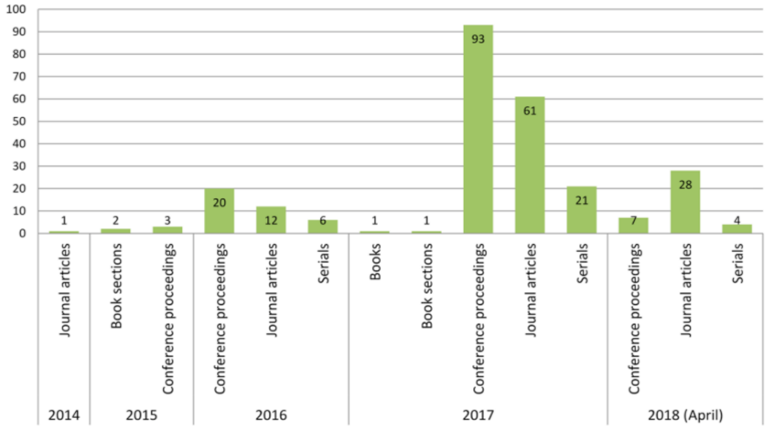

Figure 1. Year-wise analysis of the selected literature per type of publication (Casino *et al*., 2019 [9])

Each of the literature reviews mentioned above provides a clear understanding of how blockchain technology is implemented in their respective industry. Ali *et al.* [10] explained how blockchain can be implemented in various IoT in the information technology (IT) industry where focusing is more on security, privacy and trust, which is the core of blockchain technology but did not mention how it can be implemented in Malaysia in terms of governance and compliance. Furthermore, he also mentions that the current security model is no longer sufficient due to scalability, increasing hardware cost, performance and power consumption.

Guin *et al*. [11] using a blockchain authentication scheme. The researcher proposed suitable architecture for IoT that includes a security protocol algorithm. It does not mention a specific industry for the architecture; thus, one must know security algorithms to apply the architecture. The researcher also highlights that the proposed architecture is a novel, secured, but low-cost communication device for authentication.

While [11] focuses on architecture, Li *et al*. [12] proposes a blockchain authentication system model. In this model, the researcher discussed high-level functions for each item in the model. The researcher also mentions a suitable deployment environment and the use of Merkle root hash for data integrity [13]. The researcher uses Raspberry Pi with open source project hyperledger fabric as their prototype blockchain network to verify the proposed model. The researcher also provides performance analysis such as throughput and delay, which fellow researchers can implement and understand the drawback.

Folkinshteyn and Lennon [14] uses technology acceptance model (TAM) for bitcoin, which uses blockchain technology. The researcher proposed TAM factors for two groups which are internal and external. This includes acceptance from the developer and customer. The proposed TAM model is specific to bitcoin, suitable for digital banking. The researcher also includes the federal and state regulation for the case study, which help other researchers to understand the acceptance by compliances and regulators.

Natoli and Gramoli [15] discussed the disadvantages of blockchain technology and used Nakamoto's consensus and smart contracts to identify blockchain anomalies. The researcher reproduced the anomalies using a prototype in the ethereum network. Furthermore, it is not advisable to use blockchain systems unless the researcher fully understands blockchain's underlying design and principles [15]. The discouragement is one of the drawbacks of the research. It will be more beneficial if the researcher can provide alternate solutions to their discovered anomalies.

Herian [16] discussed the acceptance level of blockchain technology in general. The author mentioned the regulatory and political points of view in blockchain technology. The understanding and acceptance of blockchain technology are dependent on the regulatory acceptance that will change the socio-economy in terms of community and working environment [16]. This article proves that regulatory and compliances are the culprit that is taking a step backwards in the blockchain technology evolution. This will benefit the researcher in understanding how the acceptance of blockchain technology can be related to regulatory and compliance effectiveness in providing guidelines.

Table 1. Literature review on blockchain authentication technology

Authors (Year)	Focus
Ali *et al*. [10]	Proposed IoT-blockchain architecture focused on critical factors such as confidentiality, integrity, latency, and availability
Guin *et al*. [11]	Proposed authentication scheme using blockchain technology using global blockchain instance (smart contract and key-value store)
Li *et al*. [12]	Design and implement a prototype of blockchain authentication using open-sourced platform hyperledger fabric
Folkinshteyn and Lennon [14]	Technology acceptance model for cryptocurrency. Identified perceived ease of use (PEU) and perceived usefulness (PU) for blockchain technology
Natoli and V. Gramoli [15]	Execute and experiments on building author's private blockchain–identify key factors that simplified blockchain technology implementation
Herian [16]	Study on issue and challenges in the regulation of blockchain–provide perspective on regulatory authorities and governments to ensure democratic accountability and regulatory legitimacy within the blockchain ecosystem
Oh and Shong [17]	Discussed a few implementations of blockchain, including JB Bank of Korea. It emphasizes the method of authentication used by the bank to simplify the authentication method

3. RESEARCH METHOD

This research was conducted using the database from ResearchGate, IEEE, UITM online journal library, and Google Scholar in terms of the data collection method. The Boolean keywords searching method can produce accurate information retrieval [18]. Thus, the keywords used for the search are "blockchain technology", "blockchain authentication technology", and "secured technology in the financial industry". Fifty-three (53) papers were found related to blockchain technology. Twenty-five (25) papers were selected as they were most suitable for blockchain technology and authentication technology for banking and FI. In addition, the literature study identified terms such as elements, factors, and components that other researchers mentioned.

For the data analysis method, the researcher used the content analysis method of deductive category application [19]. All the subtopics mentioned by other researchers ranging from "security risk" to "technology complexity" were coded into "adoption factors" [20]. Then the detailed explanation in the research paper was grouped based on the researcher's understanding of their nature into their respective components as "keywords". The resemblance between the "keywords" between each research paper was also identified. It helps the researcher group all the keywords identified to each "adoption factor". The adoption factors are then used to describe all the characteristics for each component.

The discovered adoption factors were used as key elements to analyze RMiT guidelines from the Central Bank of Malaysia (BNM). In addition, the content analysis method was also being used whereby the quotation from the RMiT guidelines will be coded based on nature and characteristic into "characteristic". A guidelines model consisting of adoption factors and characteristics was developed from the analysis to align the findings in the literature review and RMiT guidelines. This result was then discussed to understand the alignment in implementation in banking and FI in Malaysia.

4. RESULTS AND DISCUSSION

Based on the literature study, the words "element", "factor", and "component" were mentioned in the literature study used as "keywords" in Table 2. The researcher then decided to group similar elements into unique adoption factors. The adoption factors identified above in Table 2 analyzed RMiT guidelines. The researcher decided that the subtopic for each policy in RMiT guidelines is suitable to be adopted as a characteristic. The characteristics are then mapped with the "adoption factors" component based on the nature of the characteristics. The number column represents the subtopic numbering in RMiT guidelines, and the quotation column represents each subtopic in the RMiT guidelines. A guideline model will be proposed based on RMiT guidelines. Characteristics for "security risk", "technology latency", "regulatory support" and "technology complexity" have been mentioned a few times, but "implementation cost" was never mentioned. All the mentioned components were accepted as "adoption factors" except "implementation cost". As a conclusion, the finding suggested that four (4) components will be accepted as "adoption factors" while "implementation cost" then will be dropped from the model. The result is shown in Table 3. Based on the findings from Table 2, the "Adoption Factors" were then developed based on "component" and "characteristics" gathered from the RMiT policy. Finally, the research model was developed that reflects the findings. Figure 2 shows the research model for the adoption of Blockchain technology. Details explanation on the adoption factors alignment with RMiT policy refers as below. The similarity from the literature study indicates that the characteristics were matched with the RMiT policy.

Table 2. Adoption factors of blockchain authentication technology

Keywords	Authors	Adoption factors
Cryptography Data Integrity	Ali *et al.* [10] Guin *et al.* [11] Li *et al.* [12] Folkinshteyn and Lennon [14] Kiktenko [21]	Security risk
Processing time Turnaround-time	Folkinshteyn and Lennon [14] Natoli and V. Gramoli [15]	Technology latency
Regulatory standard Compliance requirement	Herian [16]	Regulatory support
Infrastructure cost Lower cost in record keeping Open-source	Guin *et al.* [11] Li *et al.* [12] Hammi *et al.* [22]	Implementation cost
Simplify process API availability Common language Free participation	Folkinshteyn and Lennon [14] Khairuddin *et al.* [23]	Technology complexity

Table 3. Finding from data analysis method

From literature study	Characteristics	No of the times mentioned in RMiT guidelines	In refined model
Security risk	Cryptography	3	Accepted as component
	Access control	3	
	Security of digital services	5	
Technology latency	Network resilience	2	Accepted as component
	Data centre operation	1	
	Data centre infrastructure	1	
Regulatory support	Notification of technology-related application	1	Accepted as component
	Assessment & GAP analysis	1	
Technology complexity	Technology operation management	1	Accepted as component
	System development	4	
Implementation cost	Not available	0	Dropped

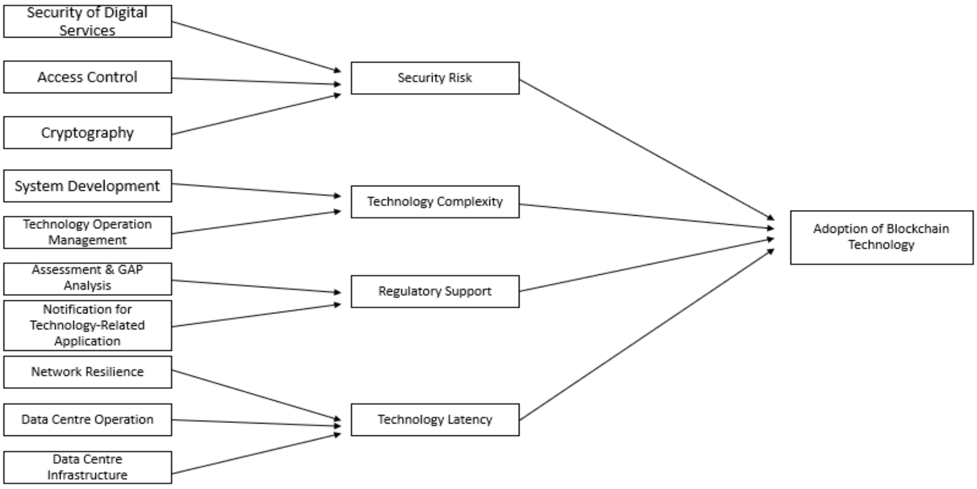
Security of Digital Services
Access Control
Cryptography
System Development
Technology Operation Management
Assessment & GAP Analysis
Notification for Technology-Related Application
Network Resilience
Data Centre Operation
Data Centre Infrastructure
Security Risk
Technology Complexity
Regulatory Support
Technology Latency
Adoption of Blockchain Technology

Figure 2. Research model for adoption factors of blockchain technology

4.1. Security risk

The key to online transactions is trust. In order to gain trust, banking and FI must ensure the blockchain authentication technology is secured enough to prevent fraudsters and scammers from being able to manipulate and gain access to the blockchain network. Most of the literature mentioned that security-related issues must be enforced properly [24]. Data integrity is critical to maintaining the consistency and trustworthiness of data. Only authorized personnel can modify the stored data [10]. In comparison, cryptography is the tool of authentication used in securing information in the block of a blockchain [11]. While in RMiT guidelines, "cryptography", "access control", and "security of digital services" were mentioned eleven (11) times. This indicates that security risks were the most critical factors in blockchain technology adoption.

4.2. Technology latency

In order to create a safe and secured environment, the authentication process will require a certain number of seconds to be completed [25]. For blockchain authentication technology to succeed, the implementor must understand the appropriate processing time [14]. Therefore, in RMiT guidelines, "network resilience", "data centre operation" and "data centre infrastructure" were mentioned three (3) times. There is a similarity between past researchers and the RMiT guidelines to ensure the infrastructure is robust, reliable and scalable.

4.3. Regulatory support

In banking and FI, central bank acknowledgement is a must. While in Malaysia, new technology implementation must be presented to the Central Bank of Malaysia (BNM) to obtain approval. BNM has been working with various entities on Blockchain and distributed ledger technology which will help to obtain acceptance from regulatory bodies [26]. Moreover, Herian [16] mentioned that critical government law, regulatory and compliance must participate and take responsibility for blockchain technology to thrive. Thus, in the RMiT policy, every new technology required BNM to be notified under the characteristic of "Notification of technology-related application". This ensures that the new technology has been verified and covered all gaps under "Assessment and GAP analysis".

4.4. Technology complexity

Nowadays, most systems and technology prefer the application programming interface (API) for better connectivity between different ecosystems [27]. The availability of open-source and community forums will help reduce the level of development complexity, thus will gain acceptance from management and technical perspective [14]. Furthermore, the simplification of the process and the usage of common language did help in the ease of developing a physical prototype [23]. Li *et al*. [12] explained that using hyperledger fabric is easy due to free participation and easy access to information. Secured authentication is one of the most important success elements for online banking and transactions, and it has become something of a leap of faith for many people [1], [28]. In part, this is because banking and financial institutions (FI) themselves place a high value on trust as the foundation of their customer relationships [2], [29]. The research model can be used for future researchers to construct hypotheses for data analysis to obtain statistical data. Based on Figure 3, the "adoption factors" were then developed based on "component" and "characteristics". The inner ring indicates the "components", and the outer ring indicates the "characteristics" shown in Figure 3.

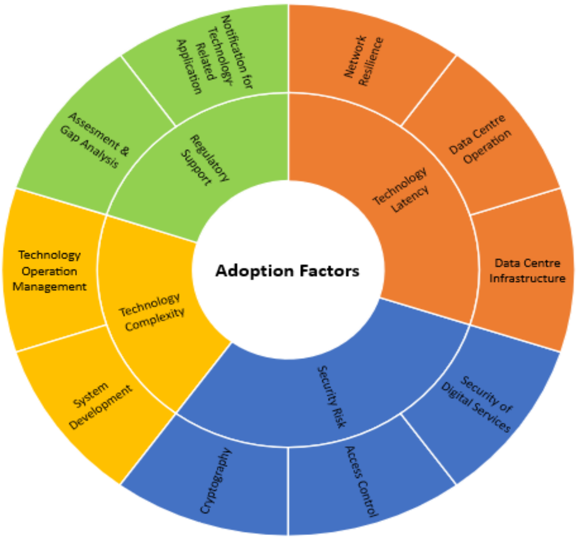

Figure 3. Adoption factors for blockchain authentication technology in banking and FI

5. CONCLUSION

Blockchain technology is an emerging technology for banking and FI in Malaysia. Therefore, identifying factors and key elements is essential to measure the viability of blockchain technology adoption. This study examines the adoption factors that influence technology adoption for Blockchain authentication technology. The components were then mapped with the RMiT policy document by BNM to ensure the feasibility to be adopted in banking and FI in Malaysia. The proposed adoption factors contain the component known as "security risk", "technology latency", "regulatory support", and "technology complexity". It will be critical for the implementer to consider the adoption factors to mitigate any obstacle during implementation. The disadvantage of this study is that the adoption variables were provided exclusively for banking and FI in Malaysia. Different countries' central banks will have different policies. The researcher might broaden the criteria to incorporate audit and compliance findings, risk factors and assessment, and infrastructure architecture for future tasks. The relationship between adoption factors in accomplishing technology adoption carries distinct viewpoints in each bank; consequently, the recommendation can provide more value to the adoption factors. Based on the findings, adoption factors can be implemented in project implementation, particularly for those directly involved in Blockchain authentication technology.

REFERENCES

[1] Z. Xu, Q. Wang, Z. Wang, D. Liu, Y. Xiang, and S. Wen, “PPM: a provenance-provided data sharing model for open banking via blockchain,” in *Proceedings of the Australasian Computer Science Week Multiconference*, Feb. 2020, pp. 1–8, doi: 10.1145/3373017.3373022.

[2] T. Pikkarainen, K. Pikkarainen, H. Karjaluoto, and S. Pahnila, “Consumer acceptance of online banking: an extension of the technology acceptance model,” *Internet Research*, vol. 14, no. 3, pp. 224–235, Jul. 2004, doi: 10.1108/10662240410542652.

[3] N.-M. Yaghoubi and E. Bahmani, “Factors affecting the adoption of online banking-an integration of technology acceptance model and theory of planned behavior,” *International Journal of Business and Management*, vol. 5, no. 9, pp. 159–165, Aug. 2010, doi: 10.5539/ijbm.v5n9p159.

[4] Y. Cai and D. Zhu, “Fraud detections for online businesses: a perspective from blockchain technology,” *Financial Innovation*, vol. 2, no. 1, p. 20, Dec. 2016, doi: 10.1186/s40854-016-0039-4.

[5] Y. Guo and C. Liang, “Blockchain application and outlook in the banking industry,” *Financial Innovation*, vol. 2, no. 1, p. 24, Dec. 2016, doi: 10.1186/s40854-016-0034-9.

[6] R. Kumar, M. F. Tahir, S. Kumar, A. Zia, H. Memon, and W. Mahmood, “Challenges in adoption of blockchain in developing countries,” in *2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST)*, Dec. 2019, pp. 1–8, doi: 10.1109/ICEEST48626.2019.8981674.

[7] Z. Haddad, M. M. Fouda, M. Mahmoud, and M. Abdallah, “Blockchain-based Authentication for 5G Networks,” in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020*, Feb. 2020, pp. 189–194, doi: 10.1109/ICIoT48696.2020.9089507.

[8] “Risk management in technology (RMIT) - bnm.gov.my.” [Online]. Accessed: 21 Apr 2022 Available: https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf

[9] F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: current status, classification and open issues,” *Telematics and Informatics*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[10] J. Ali, T. Ali, S. Musa, and A. Zahrani, “Towards secure IoT communication with smart contracts in a blockchain infrastructure,” *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 10, pp. 578–585, 2018, doi: 10.14569/IJACSA.2018.091070.

[11] U. Guin, P. Cui, and A. Skjellum, “Ensuring proof-of-authenticity of IoT edge devices using blockchain technology,” in *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree*, Jul. 2018, pp. 1042–1049, doi: 10.1109/Cybermatics_2018.2018.00193.

[12] D. Li, W. Peng, W. Deng, and F. Gai, “A blockchain-based authentication and security mechanism for IoT,” in *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, Jul. 2018, vol. 2018-July, pp. 1–6, doi: 10.1109/ICCCN.2018.8487449.

[13] M. S. Niaz and G. Saake, “Merkle hash tree based techniques for data integrity of outsourced data,” in *27th GI-Workshop on Foundations of Databases (Grundlagen von Daten-banken)*, 2015, vol. 1366, pp. 66–71.

[14] D. Folkinshteyn and M. Lennon, “Braving bitcoin: a technology acceptance model (TAM) analysis,” *Journal of Information Technology Case and Application Research*, vol. 18, no. 4, pp. 220–249, Oct. 2016, doi: 10.1080/15228053.2016.1275242.

[15] C. Natoli and V. Gramoli, “The blockchain anomaly,” in *Proceedings - 2016 IEEE 15th International Symposium on Network Computing and Applications, NCA 2016*, Oct. 2016, pp. 310–317, doi: 10.1109/NCA.2016.7778635.

[16] R. Herian, “Taking blockchain seriously,” *Law and Critique*, vol. 29, no. 2, pp. 163–171, Jul. 2018, doi: 10.1007/s10978-018-9226-y.

[17] J. Oh and I. Shong, “A case study on business model innovations using Blockchain: focusing on financial institutions,” *Asia Pacific Journal of Innovation and Entrepreneurship*, vol. 11, no. 3, pp. 335–344, Dec. 2017, doi: 10.1108/APJIE-12-2017-038.

[18] M. B. Aliyu, “Efficiency of Boolean search strings for information retrieval,” *American Journal of Engineering Research (AJER)*, vol. 6, no. 11, pp. 216–222, 2017.

[19] P. Mayring, “A companion to qualitative research,” *FORUM Qualitative Social Research Sozialforsch*, vol. 1, pp. 851–855, 2000.

[20] K. A. Kamaruddin and N. MdNoor, “Citizen-centric demand model for transformational government systems,” *Proceedings of Pacific Asia Conference on Information Systems (PACIS) 2017*, 2017.

[21] E. O. Kiktenko *et al.*, “Quantum-secured blockchain,” *Quantum Science and Technology*, vol. 3, no. 3, p. 035004, Jul. 2018, doi: 10.1088/2058-9565/aabc6b.

[22] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, “Bubbles of trust: a decentralized blockchain-based authentication system for IoT,” *Computers and Security*, vol. 78, pp. 126–142, Sep. 2018, doi: 10.1016/j.cose.2018.06.004.

[23] I. E. Khairuddin, C. Sas, and C. Speed, “BlocKit,” in *Proceedings of the 2019 on Designing Interactive Systems Conference*, Jun. 2019, pp. 1449–1462, doi: 10.1145/3322276.3322370.

[24] M. Aboelmaged and T. R. Gebba, “Mobile banking adoption: an examination of technology acceptance model and theory of planned behavior,” *International Journal of Business Research and Development*, vol. 2, no. 1, pp. 35–50, Mar. 2013, doi: 10.24102/ijbrd.v2i1.263.

[25] D. Guegan and C. Hénot, “A probative value for authentication use case blockchain,” *HAL Open Science*, pp. 1–21, 2018.

[26] MyGovernment, “Blockchain and distributed ledger technology (DLT) initiatives in Malaysia 2019,” *MyGovernment*, 2019. Accessed: 21-Apr-2022. [Online]. Available: https://www.malaysia.gov.my/portal/content/30633

[27] S. Schwichtenberg, C. Gerth, and G. Engels, “From open API to semantic specifications and code adapters,” in *Proceedings - 2017 IEEE 24th International Conference on Web Services, ICWS 2017*, Jun. 2017, pp. 484–491, doi: 10.1109/ICWS.2017.56.

[28] W. Hassan, T.-S. Chou, O. Tamer, J. Pickard, P. Appiah-Kubi, and L. Pagliari, “Cloud computing survey on services, enhancements and challenges in the era of machine learning and data science,” *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 9, no. 2, p. 117, Aug. 2020, doi: 10.11591/ijict.v9i2.pp117-139.

[29] M. O. Adebiyi, R. O. Ogundokun, A. I. Nathus, and E. A. Adeniyi, “Smart transit payment for university campus transportation using RFID card system,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 5, p. 4353, Oct. 2021, doi: 10.11591/ijece.v11i5.pp4353-4360.

BIOGRAPHIES OF AUTHORS

Amir Aizzat Basori is a BSc in Netcentric Computing from Universiti Teknologi MARA in 2011 and pursued MSc in Strategic Information System with Business Management in 2020. He is currently working at Affin Bank Berhad as a Digital Banking and System Integration Manager (VP). He has 11 years of experience in banking, financial institutions, and information technology. He can be contacted at e-mail: amiraizzat.basori@gmail.com.

Nor Hapiza Mohd Ariffin is a BSc Hons in Computer Science in 1994, an MSc in information technology (IT) in 2001, and a Ph.D. in Information Systems in 2010. Her research interests are customer relationship management (CRM), strategic information system planning (SISP), human capital, spiritual information systems, online distant learning, and blockchain. Since 1995, she has been employed as a Senior Lecturer at UiTM Malaysia. She can be contacted at e-mail: hapiza@uitm.edu.my.