Asia Pacific Journal of Emerging Markets, Vol. 7, No. 2, 2023 ISSN: 2706-5634

BLOCKCHAIN'S OPPORTUNITY IN PROTECTING TRANSACTIONS AND INFORMATION IN MALAYSIAN BANKS

Fong Jun Yi
Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia.
joeyfjy1183@yahoo.com

Mohd Karim Abdul Majed
Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia.
karim.abdulmajed@apu.edu.my

Hafinaz Hasniyanti Hassan
Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
hafinaz.hasniyanti@apu.edu.my

ABSTRACT

In recent years, there has been widespread interest in applying blockchain technology to the financial sector. The primary objective of this study is to investigate the potential of blockchain technology for securing banking transactions and data in Malaysia. The study thoroughly examined the measures currently implemented in the Malaysian banking sector and how blockchain technology could improve them. This study used primary data and three variables that provide opportunities for blockchain technology: transparency, security, and consistency. The survey considered the opinions of 104 sample respondents regarding Blockchain implementation. All information is obtained from the bank's experts. In addition, the study utilized the Statistical Package for the Social Sciences (SPSS) to evaluate the relationship between three variables that can influence Malaysian banks' implementation of blockchain technology to secure information and transactions. All variables, including transparency, security, and consistency, were found to have a significant relationship with implementing blockchain technology in Malaysian banks. The study's findings shed light on the viability of implementing blockchain technology in Malaysia's banking industry and its potential impact on the sector. Overall, the study aims to educate banks about blockchain technology and enhance the technology's role in Malaysia's banking industry regarding security and privacy.

Keywords: Blockchain; Malaysian Banks; Transparency; Security

Reference to this paper should be made as follows: Yi, F. J., Abdul-Majeed, M. K. & Hassan, H. H. (2023). Blockchain's Opportunity in Protecting Transactions and Information in Malaysian Banks. *Asia Pacific Journal of Emerging Markets, 7*(2), 102-118.

Biographical Notes: Fong Jun Yi is a Research Scholar at the Asia Pacific University of Technology and Innovation, Malaysia.

Mohd Karim Abdul Majed is a Research Scholar at the Asia Pacific University of Technology and Innovation, Malaysia.

Hafinaz Hasniyanti Hassan is a Senior Lecturer at the Asia Pacific University of Technology and Innovation, Malaysia. Her areas of teaching and research interests are corporate finance, Time series Finance and econometrics.

1. INTRODUCTION

A blockchain is a type of distributed ledger that is made up of a digital combination of transactions that are monitored and recorded in a decentralized network. It is not centrally controlled, and no single person or entity influences the network's capacity to disrupt it. A blockchain comprises various data blocks, each of which holds a record of information. By connecting them, managing all information transactions ensures that records cannot be tampered with. This improves people's confidence in the network. Blockchain technology can lower transaction costs while improving transaction efficiency and speed (Likos, 2021). Over time, new technology has become important in transforming economic and social systems, thus attracting the attention of many enterprises and international organizations. Blockchain is an emerging technology with significant business advantages (Dicuonzo et al., 2021). For the banking industry, blockchain technology is the core underlying technology. Economic revolution, Internet expansion, and financial innovation have forced the banking industry to transform urgently to find new ways to increase company (Guo & Liang, 2016). According to Deloitte's 2018 Global Blockchain Survey, 34% of organizations polled had already started adopting blockchain technologies, with another 41% planning to do so in the future year (Deloitte, n.d.). Since 2015, blockchain has received great attention in the field of fintech. The system includes distributed data storage, point-to-point transmission, consensus procedures, and encryption methods. A distributed ledger is a shared, duplicated, and synchronized database among network members. It keeps track of network participants' activities, such as assets or data exchanges. All network participants must approve all record updates or changes in distributed databases. The distributed ledger technology of blockchain has transformed how businesses conduct business transactions (Brakeville & Perepa, 2017). A peer-to-peer network is a decentralized communication model in which two nodes communicate. They do not need a central server to communicate with each other. This means that once the network has been established, participants can share and store files without intermediaries (Vermaak, 2021). In addition, one of the most interesting aspects of blockchain technology is the application of various consensus mechanisms to establish decentralized consensus. Proof-of-

work (PoW), proof of equity (PoS), or proof of delegated Interest (DPoS) are the three most common consensus algorithms for blockchain (Nick & Hoenig, 2020). Since blockchain is an ever-growing list of records, cryptography has become a way to prevent third parties from accessing or gaining access to user's private information and data. Blockchain mainly uses asymmetric key algorithms and hash functions. Cryptographic features allow blockchains to connect to other blocks securely. Hash functions can be characterized by immutable data and security (Singh, 2021).

According to Isa et al., 2015, banking institutions are the primary places for criminals to launder money, making this one of the most significant hazards for banks. Failure to correctly assess money laundering risk can result in hefty fines for financial institutions. Concerns about the impact of COVID-19, banks are also facing substantial issues in AML compliance. Due to a lack of technology, banks have to rely on manual processes for oversight. As a result, many financial institutions have low faith in their financial crime framework's compliance (Jamil et al., 2021). According to Mohamed (2020), a blockchain is a distributed ledger that records all completed transactions or digital events. All transaction records are verified by the participants' consensus of the system, and stored transactions are not deleted. As banking transaction capabilities increase, although traditional banks have very confidential systems, blockchain technology can make banking processes more transparent. Users can access complete historical data, and banks' need for trust in transactions can be reduced. Banks and regulators can also promptly act on irregularities or suspicious transactions (Hassani et al., 2018). Thus, it helps to eliminate the illegal activities of cybercriminals.

Banks hold a lot of confidential information, including bank customers' information, account status, and transaction history. Without tokens, blockchain technology can protect information security and ensure the complete confidentiality of all bank data (Popova & Butakova, 2019). Protection and security are the biggest problems brought about by the Internet and the abundance of information, and increased security can lower the risk of information and transactions on the network being infiltrated by hackers or saboteurs (Alsunaidi & Alhaidari, 2019). According to Popova & Butakova's 2019 research, the Merkle tree of the blockchain protects all transactions in the block, and the change of one transaction causes the entire block to change. Is there a relationship between security and the implementation of Blockchain? The banking system lacks perfect supervision and tracking, and agents will record false transactions intentionally or unintentionally, causing customer losses (Fan et al., 2020). The blockchain's P2P network makes consensus necessary for new transactions. Consensus mechanisms help nodes accept or reject transactions and detect transactions through validity and verification. In the operation of the blockchain, the consensus mechanism can satisfy the properties of validity and consistency to ensure the same transaction records and data (Song et al., 2021). Previous research has shown the benefit of Blockchain

in protecting bank transactions. Therefore, this quantitative study will assist in investigating the opportunity for the implementation of Blockchain technology in Malaysian banks. This research aims to investigate the relationship between the benefits of Blockchain Technology and the implementation of Blockchain in protecting transactions and information in Malaysian banks. The specific objectives are (1) to study the relationship between transparency and implementation of Blockchain in Malaysian banks, (2) to examine whether there is a relationship between security and implementation of Blockchain in Malaysian banks, (3) to determine the relationship between consistency and implementation of Blockchain in Malaysian banks.

2. LITERATURE REVIEW

Blockchain, distributed ledger technology, allows users to ensure low-cost settlement, permitting transactions and asset transfers (Tschorsch & Scheuermann, 2016). It is the leading technology of cryptocurrencies and has been used in various fields, including financial cryptocurrencies (Chen et al., 3 C.E.). Distributed ledgers and blockchain technologies have advanced significantly in banking (Kashyap & Saurav, 2021). Guo & Liang (2016) stated that blockchain can help credit institutions automatically record vast amounts of data while also offering "know your customer" (KYC), which allows banks to store client information in a database and then enter it into the blockchain using encryption technology. Furthermore, encryption technology can provide a consensus mechanism, ensuring that the information in the digest is consistent with the original data and preventing incorrect information from spreading among peers. For a transaction to be considered valid, it must be agreed by consensus among nodes in a P2P network (Koteska et al., n.d.). Through the ledger of transaction records, the blockchain network nodes can preserve the security and accuracy of information. Miners must employ a hash function to solve arithmetic problems before creating a new block to verify all transactions. New blocks will surface across the blockchain network, and all nodes will share the same full ledger. Clearly stated, blockchain is a decentralized ledger with a reliable ledger. In addition, according to Mohamed's (2020) research, blockchain features global remittances, smart contracts, automated bank ledgers, and digital assets that help traditional banks improve transparency, trust, and privacy issues. Despite blockchain's numerous benefits, it faces several technological, regulatory, and adoption obstacles. In Malaysia, blockchain technology is still in beta, and research (Koteska et al., n.d.) found that blockchain transaction speeds are slow. For banks, transaction timing is a key concern. All network nodes must confirm every transaction on the blockchain, slowing down transactions and lowering performance. Moreover, the deployment of blockchain technology in the banking industry is allegedly hampered by decentralization. Many banks will form the blockchain alliance R3 to suit varied needs, according to Guo and Liang (2016), since the financial sector often requires a certain degree of centralization to assure security. However, American Express implements Ripple's blockchain-based quick payments. Mohamed's (2020) research shows that the banking and financial

industry no longer views blockchain technology as a danger because the world's largest banks are also studying blockchain for opportunities.

2.1 Transparency

Bushman (n.d.) found that transparency serves a vital corporate governance function in all industries, with its components working together to generate, gather, and verify information and communicate it to players other than banks. External stakeholders have access to timely and accurate data on the bank's regular performance, financial position, business model, governance, and risks. Transparency and disclosure are vital for banks, according to the literature. Banks can distort or obscure misleading information when lacking transparency and disclosure (Ratnovski, 2013). According to Miraz et al. (2021), transaction transparency is a corporation's trustworthiness to end users, and a lack of transaction openness would lower customer trust and company performance. According to Mensah's (2021) study, public disclosure of both information and regulatory information can help to improve the banking system's safety and soundness, and the more transparency, the better market participants' ability to promote safe and sound banking. Data in financial statements might be affected if institutions are reluctant to reveal transparent information or postpone disclosure. Transparency of information cannot rely primarily on the action of authorities but also on elements such as company leaders' initiative (Nguyen et al., 2020).

Xu et al. (2019) stated that the benefits of blockchain include information transparency and openness. As a distributed ledger system, blockchain allows for verifying new data and removing central authority, both of which are critical in the banking business 11 (Kashyap & Saurav, 2021). The blockchain's distributed ledger technology assures that user information has not been tampered with (Beck et al., 2016). Beck et al. (2016) state that blockchain can eliminate uncertainty, insecurity, and ambiguity in-network participant transactions by enabling complete disclosure. One of the most important characteristics of blockchain is trust. Everyone can access the information in the ledger because the whole blockchain code is open, and everyone can access the information in the ledger, reducing the chance of back doors or amendments. The terms public and shared interactions explain the transparency trust provides in blockchain technology (Ali et al., 2020). Since the publicly observable transactions provided by distributed ledger technology systems cannot meet the core criterion of a wholesale payment system to keep all transactions secret, Río (2017) asks whether DLT can achieve the advantage of more elasticity while the transactions remain private. However, the notary-based DLT system allows for greater anonymity, resulting in a lack of transparency; no node can own all the information. Therefore, transparency and privacy still have certain limitations. H1: There is a relationship between transparency and the implementation of Blockchain in protecting transactions and information in Malaysian banks.

2.2 Security

Bank information security means that the bank information system's hardware, software, and data are protected from being easily damaged, altered, or leaked. According to Shrinath (1997), information is reflected in the banking industry. Since the 1990s, IT and banking have had a close association, and IT management is all about keeping information safe. Many large banks are vulnerable to the risk of security failures. Information security includes managing and maintaining the integrity of an organization's information and the management and assurance of information in electronic form. This is the introduction of high-tech innovations in the banking industry to enhance competitive advantage and reduce impact. There is a direct relationship between security information and the performance of banking operational risk (Bojinov, 2017).

Blockchain systems include private and public blockchains. Authorized nodes verify transactions on a private blockchain, and the owner has the highest authority to 12 control node access. Although the public blockchain has full public access, the user's real identity will not be exposed, and anonymity will be high. Permissioned blockchains combine private and public blockchains, where nodes are rigorously inspected and overseen, restricting access to participants and data on the ledger (Viriyasitavat & Hoonsopon, 2019). Garg et al. (2020) discovered that when data is stored in the blockchain, it is tough for network participants to make changes or transformations, enhancing the security of the technology. In banking, blockchain brings opportunities for decentralized platforms, secure record-keeping, and fast transaction systems (Jaag & Bach, 2017). Cryptography is the process of encoding data to ensure its confidentiality. The blockchain hash algorithm is an encryption method that can assure data sharing security and privacy (Chen et al., 2022). Bello Alhaji Buhari et. Al. uses the MD5 cryptographic hash function to encrypt the details in the database and must be authorized to read the information (Khudhur et al., 2018). While blockchain solves banks' management and auditing problems, some security challenges remain. Hackers may steal keys and attack the ledger's system. Flawed code raises risks for banks, businesses, etc., and vulnerabilities in security systems prevent blockchain technology from functioning correctly (Garg et al., 2020).

2.3 Consistency

The expectation that information from all sources is consistent is considered consistency (Raja, 2016). According to Currie (2018), consistency is the most important characteristic of banks. Every piece of data in any microservice system will be duplicated. When the duplicate and the original information are not identical, problems can develop. Users and banks will gain trust because of consistency, which will benefit society and industry. Business transactions slow significantly when there is a lack of consistency. As a result, society's cornerstones are trust and consistency. According to Park (2020), trust

plays a vital role in financial development. The greater a user's or business's trust in a bank, the more eager they are to transact with it. Blockchain utilises software algorithms from distributed consensus protocols to verify each transaction and assure the immutability of transaction records in the blockchain. Immutability also offers the advantage of retaining a history of each transaction record, ensuring high integrity. Since each block in the ledger will be linked by an encryption algorithm, a valid transaction will be formed. The integrity provided by the distributed peer-to-peer ledger system can ensure that the data stored in the chain can be consistent and not easily tampered with (Gietzmann & Grossetti, 2021). The Consensus Mechanism (CM) is an essential technology in blockchain. Nodes are generated according to preset regulations, and all assigned nodes must reach a consensus on the transactions in the data. Examples of CMs are Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). These mechanisms can guarantee the consistency and authenticity of the blockchain (Carrara et al., 2020). (Garg et al., 2020) because of the consensus technology, blockchain can increase confidence among professional partners by allowing them to rely on trustworthy records and solid security architecture, increasing the implementation of blockchain technology. Popova and Butakova (2019) concluded that blockchain helps improve the storage, synchronization, loss, and integrity of data in the database because its technology is fully synchronized. On the other hand, Reyna et al. (2018) said that 51% of attacks remain a hazard in consensus procedures. When a blockchain participant controls more than 51% of the mining power, he or she can control the network's consensus. Participants can disrupt others to generate new blocks, and attackers can earn rewards for their strategies. The entire consensus system will be out of control and vulnerable.

3 DATA AND METHODOLOGY

The quantitative research study will use a questionnaire for primary data collection. The two main methods for distributing questionnaires are the Internet and mobile phones (Akram et al., 2019; Aslam et al., 2022). Social media platforms such as Facebook, Instagram, and Microsoft Teams are used to connect with desired audiences. The sample size for this study is 104 respondents.

3.1 Reliability Test

This study uses Cronbach's Alpha reliability test. Table 1 shows the alpha values for all variables, including implementation of blockchain technology, transparency, security, and consistency, which are 0.895, 0.881, 0.883, and 0.880, respectively. From the above, we know that the alpha values of all variables are between 0.7 and 0.95, so they are acceptable within Cronbach's alpha range. Finally, the overall Cronbach's Alpha for all variables is 0.952, which is a bit high in the range but still acceptable.

Table 1: Cronbach's Alpha

Variables	Value
Independent Variables	
Transparency	0.881
Security	0.883
Consistency	0.880
Dependent Variable	
Implementation of Blockchain	0.895
Overall Cronbach's Alpha	0.952

3.2 Descriptive Statistics

From Table 2, the values of all variables are acceptable since the variables have skewness between -2.0 and +2.0 and kurtosis between -7 and +7. First, the dependent variable, the blockchain implementation, has a skewness statistic of -1.587 and a kurtosis statistic of 2.904, suggesting that both are acceptable. The skewness and kurtosis of transparency are favored, as it has a skewness statistic score of -1.437 and a kurtosis score of 1.970. Furthermore, security has a skewness of -1.695 and a kurtosis of 3.797, while blockchain consistency has a skewness of -1.361 and a kurtosis of 2.377. Finally, the security of the blockchain is the most crucial variable in this questionnaire, as it has the highest average value of 4.2320 and the lowest average value of 4.1799 for blockchain consistency.

Table 2: Descriptive Analysis

Variables	Min	Max	Mean	Std Deviation	Skewness		Kurtosis	
					Statistic	Std.Error	Statistic	Std. Error
Implementation of Blockchain	1.67	5.00	4.1939	0.68742	-1.587	0.237	2.904	0.469
Transparency	1.88	5.00	4.2224	0.67054	-1.437	0.237	1.970	0.469
Security	1.63	5.00	4.2320	0.61937	-1.695	0.237	3.797	0.469
Consistency	1.71	5.00	4.1799	0.65116	-1.361	0.237	2.377	0.469
Valid N=104								

3.3 Correlation Coefficient

With a value of 0.832, the use of blockchain technology in banks has a strong positive correlation with transparency. This means that transparency is 83.2% dependent on blockchain technology. The p-value (significant value) is less than 0.001, indicating that the correlation is highly significant because it is less than the threshold of 0.05. The correlation coefficient, r, between the independent variable, security, and the dependent variable, blockchain technology implementation, is 0.863. This suggests a positive correlation, with security being 86.3% related to blockchain technology implementation. Furthermore, the p-value is less than 0.001, indicating a highly significant correlation because it is less than 0.05. The correlation results for consistency

and blockchain technology implementation show a positive correlation, with r = 0.833. Furthermore, the p-value is 0.001, indicating statistical significance when the p-value is less than 0.05.

Table 3: Pearson's Correlation Analyses

		DV	IV1	IV2	IV3
DV	Pearson Correlation	1	.832**	.863**	.833**
	Sig. (2-tailed)		<.001	<.001	<.001
	N	104	104	104	104
**. Correlation is significant at the 0.01 level (2-tailed).					

DV = dependent variable (implementation of blockchain)
IV1= first independent variable (transparency)
IV2 = second independent variable (security)
IV3 = third independent variable (consistency)

3.4 Multiple Linear Regression

R in Model Summary is the multiple correlation coefficient between three or more variables. The R-value range is from -1 to +1, showing the positive or negative relationship between the dependent and independent variables. There is a miscorrelated to all variables when the R-value is 0. Moreover, R-squared is calculated as (Multiple R)^2 and represents the percentage of variance in the multiple linear regression model that predicted variables can cover. The R-square value is often used in practice since it estimates the predictor variable's accuracy in predicting the response variable's value (Zach, 2021). Table 4 shows the correlation coefficient R-value of 0.899, showing a positive correlation between all variables. Additionally, the value of R2 is 0.808, indicating that 52 of the three independent variables in this study explain 80.8% of the dependent variable. This can also describe the independent variables, such as transparency, security, and consistency, that strongly correlate with implementing Blockchain Technology. The remaining 19.2% of blockchain technologies may be affected by other features.

Table 4: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.899[a]	.808	.803	.30544

a. Predictors: (Constant), transparency, security, consistency
b. Dependent Variable: Implementation of Blockchain Technology

Table 5: ANOVA Analysis

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	39.343	3	13.114	140.57	<.001[b]
	Residual	9.329	100	.093		
	Total	48.673	103			

a. Predictors: (Constant), transparency, security, consistency
b. Dependent Variable: Implementation of Blockchain Technology

Table 6: Regression Coefficient Analysis

Model	Unstandardized Coefficients B	Std. Error	Standardized Coefficients Beta	t	Sig.
(Constant)	-.126	.213		-.592	.555
Transparency	.246	.092	.240	2.657	.009
Security	.504	.093	.454	5.439	.000
Consistency	.275	.094	.261	2.921	.004
Dependent Variable: Implementation of blockchain technology					

This study used a statistical analysis technique (ANOVA) to compare the numerical dependent variables. It can check whether significant differences exist between the means of two or more groups. Besides that, ANOVA can be used to demonstrate whether all the variables were effective (Singh, 2018). The sum of squares represents a measure of variation or deviation from the mean. In analysis of variance (ANOVA), the total sum of squares assists in expressing the overall variation related to numerous factors. The sum of squares of the residual and the regression sum of squares is the total sum. The regression sum of squares describes how much response variability can be explained using a regression model (Minitab, n.d.). The df in the analysis of variance (ANOVA) is also known as the degree of freedom; it is calculated by subtracting 1 from the number of variables (df = n-1) (graphpad, n.d.). Analysis of variance (ANOVA) uses F-tests to evaluate the statistical equality of means. An F-value is the ratio of two variances, and it is used to test the hypotheses. Besides that, there is a significant relationship between the two variables if the significance level 53 (p-value) of ANOVA is less than or equal to 5% (p-value ≤ 0.05). The null hypothesis, H0, will be rejected (Frost, 2019). From Table 5, the df is equal to 3 (df = 4-1 = 3). It is calculated from the four variables involved in implementing Blockchain Technology: Transparency, Security, and Consistency. Also, the residuals of degree of freedom are based on a sample size of 104 responses received. From this sample size of 104, subtract 4 variables from the sample size to get 100. Next, combine the degrees of freedom with a value of 3 and the residual degrees of freedom with a value of 100 to produce a total of 103 degrees of freedom. Therefore, it can be inferred that when the sample size increases, df also increases. Besides that, the F-value can be presented in Table 5, which is 140.570, and it is calculated by using the Regression of the Mean Square divided by the Residual of the Mean Square (13.1143333 / 0.09329). The significance level in ANOVA is <.001, lower than 0.05. Hence, it shows that the dependent variable, the implementation of Blockchain technology, is significantly related to three independent variables: transparency, security, and consistency. Based on the outcome, the null hypothesis H0 should be rejected. Table 6 shows the coefficients of the results among the variables. Based on Table 6, the significant value of the variable Transparency is 0.009, security's significant value is 0.000, and consistency's significant value is 0.004. The values of these variables are considered statistically significant, which expresses that the null hypothesis is rejected since the p-value is less than 0.05. It shows that these variables, including

Transparency, Security, and Consistency, will significantly influence the implementation of Blockchain Technology in Malaysian Banks.

4 RESULTS AND DISCUSSION

This study aims to provide a deeper understanding of blockchain technology and opportunities for banks to implement the technology to protect transactions and information in Malaysian banks. Blockchain is one of the innovative areas of financial technology, and all banking businesses are very concerned about this technology. The bank's experts and management, including the general manager and financial auditors, can benefit from this research; they can learn how blockchain works and keep all the information safe and confidential. In addition, the bank's technical staff can also learn how innovative blockchain technology works and how to use it properly. This study may also allow customers to choose a more secure bank for financial services. By learning from this research, banks can more clearly protect customer transactions, and their knowledge of transparency, security, and consistency will increase. Moreover, this study can also serve as a reference for future researchers to further study the trend of blockchain for the financial industry in the future.

All three alternative hypotheses regarding the relationship between transparency, security, and consistency with implementing blockchain technology have been accepted based on the findings. In Malaysia, blockchain has proven effective in protecting bank transactions and information. Buitenhek (2016) explained that auditors and regulators can pre-enforce compliance with blockchain, allowing them to scrutinize transactions before they occur. This leads to fully transparent and real-time reporting, which benefits regulators. In addition, according to Wang et al. (2019), blockchain, as a distributed technology, can enhance the transparency and visibility of information data, serve as an unalterable ledger, and help establish customer trust in banks. A recent study by Chowdhury et al. (2021) found that banks can enhance their security by utilizing blockchain technology to exchange data through shared records. Unlike storing all data in a single database, blockchain offers higher security and protection against database assaults (Mendling et al.,2018). Researchers have also determined that blockchain can prevent information leaks and hacker theft of customer data. The article further explains that blockchain allows transactions and information to be verified through consensus algorithm calculations, which ensures that the trade data cannot be altered once confirmed. This consensus algorithm provides consistency to banks in protecting the information, making it difficult for any participant to modify the data easily. Additionally, research conducted by Guo, Y., & Liang, C. (2016) has shown that many bank transactions and information comply with blockchain consistency, allowing assessors and government officials to access the blockchain and regulate banking operations accordingly.

5 CONCLUSION

Blockchain is a technology that allows simple, efficient, and secure transactions. Ensure all bank information and transactions are stored securely and transparently through a publicly shared database. As a result, the benefits provided by blockchain have become an important factor in banks' implementation of the technology. Many commercial banks have begun to develop and apply blockchain technology to enhance the traditional centralised banking system. In many different studies, financial institutions have been found to cut out middlemen by leveraging the security, immutability, and transparency of blockchain (Underwood, 2016). It follows that there is a positive correlation between blockchain infrastructure and the chances of banks implementing blockchain. Since blockchain technology can methodically solve the whole business chain of the bank, the benefits of the blockchain are one of the important factors in increasing the bank's implementation of the blockchain. In this study, the researchers propose three benefits blockchain offers to increase the demand for blockchain in Malaysian banks. This study focuses on the features of blockchain, particularly how consistency, security, and transparency affect the opportunity of banks to implement blockchain to protect customer information and transactions. It has been discovered throughout the research process that all three of the above independent variables have a positive and significant impact on banks' transactions and information security. It may be said that the higher the level of blockchain features, the higher the opportunity for a bank to implement blockchain for protecting information and transactions. The relationship between the security variable and blockchain implementation is the most significant in this research. However, the other two variables also greatly impact how blockchain is implemented. The users should consider it. Blockchain is a fast-growing financial technology that has revolutionized how people conduct business and is driving economic reform worldwide. With the need for modernization increasing daily, people are willing to accept new technologies. Blockchain is one of the greatest and most innovative technologies, significantly changing markets and industries. Many financial giants, like large international banks, have rushed to deploy in this industry, investing many resources in technology development and experimentation. Since blockchain technology provides full transparency of information and transactions to the bank and all the participants, hence, some customers worry that their data privacy will be violated and stolen by unauthorized parties. This could prevent the widespread use of blockchain.

To address the issues of using blockchain technology, there are several recommendations to protect customers' privacy and issues in Blockchain. First, banks and users must understand blockchain cryptography and use it well. Blockchain participants can communicate using a single or pair of keys (Sahu, 2021). The key generator can set a secure password and must ensure the key is provided only to the recipient. The two parties can also reset the password after each communication. This prevents third parties from tampering or stealing any information. Users' information can also be protected with full transparency. Second, local governments can enact data privacy laws to reduce the conflict

between blockchain technology and the concept of data privacy. Government regulations could include forcing banks to implement blockchains for privacy enhancements, including ZK-SNARKS, Ring Confidential Transactions, and hybrid technologies to hide the sender's or recipient's identity and personal data (Walters & Coutu, 2022). Under the law, banks must ensure that participants confirm transactions with cryptographic proof and prevent blockchain stakeholders from arbitrarily changing personal data or disclosing information on the public blockchain. For non-compliance, stakeholders may be fined and removed from the network. Therefore, proper legal practice can reduce the risk of invasion of privacy. Finally, banks can adopt anonymous transactions to preserve customers' privacy. According to de Haro-Olmo et al. (2020), banks can use off-chain transactions to protect sensitive information, including account or credit card numbers, confidential business information, and legal information. In off-chain transactions, customer information usually has higher security and anonymity because the information details are not made public. Banks allow customers to use anonymous or pseudonyms for transactions so that the customer's information is hidden behind the public key and needs to be decrypted using the private key. In addition to ensuring information privacy, this trade can reduce transaction costs. Although blockchain technology requires obstacles and difficulties, it will be the technology leader in all industries, especially in the financial sector.

REFERENCES

Ali, O., Ally, M., & Dwivedi, Y. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. *International Journal of Information Management*, *54*, 102199.

Alsunaidi, S. J., & Alhaidari, F. A. (2019, April). A survey of consensus algorithms for blockchain technology. In *2019 International Conference on Computer and Information Sciences (ICCIS)* (pp. 1-6). IEEE.

Akram, Z., Shahid, M. N., Iqbal, Z., & Akram, H. R. (2019). How self-efficacy influences knowledge sharing and organizational citizenship behavior: a social approach form employees of pharmaceutical companies. *Indo American Journal of Pharmaceutical Sciences*, *6*(1), 643-651.

Aslam, S., Shahid, M. N., & Aftab, F. (2022). Role of entrepreneurial orientation in SMEs global performance: testing marketing strategies and technological orientation as mediators. *Journal of Marketing Strategies*, *4*(1), 173-201.

Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016). Blockchain–the gateway to trust-free cryptographic transactions. In *Twenty-Fourth European Conference on Information Systems (ECIS), İstanbul, Turkey, 2016* (pp. 1-14). Springer Publishing Company.

Brakeville, S., & Perepa, B. (2016). Blockchain basics: Introduction to business

ledgers. *Issued by IBM Corporation*.

Bushman, R. M. (2016). Transparency, accounting discretion, and bank stability. *Economic Policy Review, Issue Aug*, 129-149.

Carrara, G. R., Burle, L. M., Medeiros, D. S., de Albuquerque, C. V. N., & Mattos, D. M. (2020). Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking. *Annals of Telecommunications*, *75*, 163-174.

Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, *5*(1), 1-10.

Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M., & Cai, Z. (2022). A survey on blockchain systems: Attacks, defenses, and privacy preservation. *High-Confidence Computing*, *2*(2), 100048.

Chowdhury, M. U., Suchana, K., Alam, S. M. E., & Khan, M. M. (2021). Blockchain I am running a few minutes late; my previous meeting is running over.
application in banking system. *Journal of Software Engineering and Applications*, *14*(7), 298-311.

Currie, A. (2018, April 11). What is Eventual Consistency and Why Is It So Cool? Blog.container-Solutions.com. https://blog.container-solutions.com/what-is-eventual-consistency-and-why-is-it-so-cool.

de Haro-Olmo, F. J., Varela-Vaca, Á. J., & Álvarez-Bermejo, J. A. (2020). Blockchain from the perspective of privacy and anonymisation: A systematic literature review. *Sensors*, *20*(24), 7171.

Deloitte. (n.d.). Global Blockchain Survey | Deloitte | Energy, Resources & Industrials. Deloitte Kazakhstan. Retrieved January 26, 2022, from https://www2.deloitte.com/kz/en/pages/energy-and-resources/articles/gx-innovation-blockchain-survey.html.

Dicuonzo, G., Donofrio, F., Fusco, A., & Dell'Atti, V. (2021). Blockchain technology: Opportunities and challenges for small and large banks during COVID-19. *International Journal of Innovation and Technology Management*, *18*(04), 2140001.

Fan, W., Chang, S. Y., Emery, S., & Zhou, X. (2020, August). Blockchain-based distributed banking for permissioned and accountable financial transaction processing. In *2020 29th International Conference on Computer Communications and Networks (ICCCN)* (pp. 1-9). IEEE.

Frost, J. (2019). How to Interpret Regression Models that Have Significant Variables but a Low R-Squared-Statistics by Jim. *Statistics by Jim*.

Garg, P., Gupta, B., Chauhan, A. K., Sivarajah, U., Gupta, S., & Modgil, S. (2021). Measuring the perceived benefits of implementing blockchain technology in the banking sector. *Technological forecasting and social change*, *163*, 120407.

Gietzmann, M., & Grossetti, F. (2021). Blockchain and other distributed ledger technologies: where is the accounting?. *Journal of Accounting and Public Policy*, *40*(5), 106881.

Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial innovation*, *2*, 1-12.

Hassani, H., Huang, X., & Silva, E. (2018). Banking with blockchain-ed big data. *Journal of Management Analytics*, *5*(4), 256-275.

Isa, Y. M., Sanusi, Z. M., Haniff, M. N., & Barnes, P. A. (2015). Money laundering risk: from the bankers' and regulators perspectives. *Procedia Economics and Finance*, *28*, 7-13.

Jaag, C., & Bach, C. (2017). *Blockchain technology and cryptocurrencies: Opportunities for postal financial services* (pp. 205-221). Springer International Publishing.

Jamil, A. H., Mohd Sanusi, Z., Yaacob, N. M., Mat Isa, Y., & Tarjo, T. (2022). The Covid-19 impact on financial crime and regulatory compliance in Malaysia. *Journal of Financial Crime*, *29*(2), 491-505.

Kashyap, R., & Saurav, V. (2021). WITHDRAWN: Blockchain technology: Road to transform the Indian banking sector.

Khudhur, D. Y., Hameed, S. S., & Al-Barzinji, S. M. (2018). Enhancing e-banking security: using whirlpool hash function for card number encryption.

Koteska, B., Karafiloski, E., & Mishev, A. (2017, September). Blockchain implementation quality challenges: a literature. In *SQAMIA 2017: 6th workshop of software quality, analysis, monitoring, improvement, and applications* (Vol. 11, p. 2017).

Likos, P. (2021). How blockchain can transform the financial services industry.

Mendling, J., Weber, I., Aalst, W. V. D., Brocke, J. V., Cabanillas, C., Daniel, F., ... & Zhu, L. (2018). Blockchains for business process management-challenges and opportunities. *ACM Transactions on Management Information Systems (TMIS)*, *9*(1), 1-16.

Mensah, M. A. (2021, June). The Impact of Bank Information Transparency onCustomers' Well-Being in Ghana. https://www.researchgate.net/publication/355842109_The_Impact_Of_Bank_Information_Transparency_On_Customers'_Well-Being_In_Ghana

Miraz, M. H., Hasan, M. T., Rekabder, M. S., & Akhter, R. (2022). Trust, transaction

transparency, volatility, facilitating condition, performance expectancy towards cryptocurrency adoption through intention to use. *Journal of Management Information and Decision Sciences*, *25*, 1-20.

Nguyen, M. P., Nguyen, T. H. H., Hoang, P. D., Tran, M. D., & Pham, Q. T. (2020). Determinants Influencing Information Transparency in Vietnamese Commercial Banks. *The Journal of Asian Finance, Economics and Business*, *7*(12), 895–907. https://doi.org/10.13106/jafeb.2020.vol7.no12.895

Nick, A., & Hoenig, L. (2020). Consensus Mechanisms in Blockchain Technology. *Lexology,[Online]. Available: https://www. lexology. com/library/detail. aspx*.

Park, N. Y. (2020). Trust and trusting behavior in financial institutions: Evidence from South Korea. *International Review of Economics & Finance*, *67*, 408-419.

Popova, N. A., & Butakova, N. G. (2019, January). Research of a possibility of using blockchain technology without tokens to protect banking transactions. In *2019 IEEE conference of Russian young researchers in electrical and electronic engineering (EIConRus)* (pp. 1764-1768). IEEE.

Raja, A. (2016, July 30). Consistency and User Experience. Www.linkedin.com. https://www.linkedin.com/pulse/consistency-user-experience-amarnath-raja/

Ratnovski, L. (2013). Liquidity and transparency in bank risk management. *Journal of Financial Intermediation*, *22*(3), 422-439.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, *88*, 173-190.

Rio, D., & César, A. (2017). Use of distributed ledger technology by central banks: A review. *Enfoque Ute*, *8*(5), 1-13.

Sahu, M. (2021). Cryptography in blockchain: Types & applications. *Up Grad Blog*.

Shrinath, B. (1997). Information Security in Banks. *Journal of Financial Crime*, *5*(1), 65-71.

Singh, A. (2021, April 20). Cryptography in Blockchain Explained. Brandlitic. https://medium.com/brandlitic/cryptography-in-blockchain-explained-df11fe1bd0f7

Singh, G. (2018). A simple introduction to ANOVA (with applications in Excel). *Analytics Vidhya. Retrieved on*, *8*.

Song, H., Zhu, N., Xue, R., He, J., Zhang, K., & Wang, J. (2021). Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection. *Information processing & management*, *58*(3), 102507.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on

decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, *18*(3), 2084-2123.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15-17.

Vermaak, W. (2021). What is Peer-to-Peer (P2P) Networks? | CoinMarketCap. CoinMarketCap Alexandria. https://coinmarketcap.com/alexandria/article/what-is-peer-topeer-p2p

Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, *13*, 32-39.

Walters, N., & Coutu, S. (2022, June 9). The privacy paradox in blockchain: best practices for data management in crypto. www.dentons.com. https://www.dentons.com/en/insights/articles/2022/june/9/the-privacy-paradox-in-blockchain-best-practices-for-data-management-in-crypto.

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(11), 2266-2277.

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial innovation*, *5*(1), 1-14.

Zach. (2021, February 12). Multiple R vs. R-Squared: What's the Difference? Statology. https://www.statology.org/multiple-r-vs-r-squared