2020-1104 IJOI
http://www.ijoi-online.org/

International Journal of Organizational Innovation

BLOCKCHAIN TECHNOLOGY AND BUSINESS TRANSACTION: FROM SECURITY AND PRIVACY PERSPECTIVES

Chih-Ming Chen
Department of Finance & Economics, Fujian Business University, Fujian, China

Di-Yu Lei*
Department of Business and Management,
Ming Chi University of Technology, Taiwan.
*Corresponding Author: raymond.lei@mail.mcut.edu.tw

Jui-Hsi Cheng
College of Business & Management, Xiamen Huaxia University, P.R. China

Kai-Ping Huang
Department of Business Administration, Social Enterprise Research Center,
Fu Jen Catholic University, Taiwan.

Abstract

This study aims to analyse blockchain technology and business transaction from privacy and security perspectives. A literature review method with an Introduction and Conclusion sections have been followed for the analysis. The selected literature and their respective outcomes revealed that blockchain technology is positively associated with Cyber Security, Knowledge Sharing (KS) and Business Transaction Privacy and Security. Based on these outcomes, the positive association amid the mentioned concepts could be determined in the forms of ensuring trust among the network partners, preserving knowledge copyrights and using encryption platform based algorithms.

Keywords: blockchain, cyber security, business transaction, knowledge sharing

Introduction

Technologies in this present contemporary era have been transforming constantly due to the conduct of various business transactions and the privacy or the security issues associated with the same (Friedewald & Pohoryles, 2013). This trend is likely to continue in the future as well to make life simpler and ensure that these are accessible to every individual living in this modern world (Stepanovic, 2014). Modern technologies have already initiated in this 21st century, supporting the businesses to retain competitive-

ness and attain higher profitability levels. Some of these technologies can be recognised as “blockchain”, “machine learning” and “artificial intelligence” among others that not only alter the business landscape from the perspective of developing innovative products continuously, but also imposed significant impacts on maintaining the privacy as well as the security factor (Demirkan et al., 2020; Zhu et al., 2019). In this present-day context, remarkable efforts have been made to address and mitigate security along with privacy-related issues by better use of new generation technologies such as blockchain and Internet of Things (IoT). Conceptually, blockchain technology "applies a linked block structure to verify and store data, and applies the trusted consensus mechanism to synchronize changes in data, which makes it possible to create a tamper-proof digital platform for storing and sharing data" (Feng et al., 2019, p.45). On the other hand, IoT "is widely used in the convergence of networks through intelligent perception, recognition technology, computing, etc. Therefore, IoT is also called the third information technology revolution after the computer and the Internet" (Jiang et al., 2019, p. 185). These two identified modern technologies follow dissimilar procedures to maintain privacy and security to the maximum possible extent.

Based on the above information, this study intends to identify and analyse blockchain technology and business transaction from security and privacy standpoints. In this regard, attempts have been made to study relevant literature about blockchain technology and cybersecurity, blockchain technology and knowledge sharing and blockchain technology and business transaction privacy along with security. Considering these literature findings, three propositions have been formulated that focused on determining whether there exists a positive relationship amid blockchain technology and cybersecurity, knowledge sharing as well as business transaction privacy and security.

Literature Review and Proposition Development

Blockchain Technology and Cyber Security

According to Angelis and da Silva (2019, p.308), blockchain is described as “A secure record of historical transactions, collected into blocks, chained in chronological order, and distributed across a number of different servers to create reliable provenance”. This particular modern technology may also be defined “as a decentralized, transactional database technology that facilitates validated, tamper-resistant transactions that are consistent across a large number of network participants called nodes” (Beck et al., 2018, p.1020-1021). Kshetri (2017) highlighted that blockchain technology plays a critical function in safeguarding as well as strengthening cybersecurity by an extensive level. Justifiably, Meng et al. (2020) argued that this particular technological form is highly secured in terms of its design. For instance, under blockchain technology, there does not lay the requirement of storing any sort of data specifically with the third parties. The records of these data are being stored on several interlocked computers, which possess similar information (Mohanta et al., 2019). Therefore, if any blockchain

update of one particular computer is infringed, the system involuntarily declines it and thereby serves as better protection to cybersecurity. Based on the observation made by Hassani et al. (2018), the banking sector is the one, which has been affected by cyberattacks the most and already created a loss of nearly about USD 100 million. It is argued that the centralised nature of the operating banks eventually leads towards causing cyber attacks at large (Sengupta et al., 2020; Yang et al., 2019; Hassani et al., 2018;). Thus, this particular financial segment necessitates higher security not only to safeguard valuable data but also to cope with such monetary losses in the future. From the study findings of Yang et al. (2018), it is evident that blockchain technology holds the ability to stop cyberattacks and thereby provide utmost security to the operating banks because of its unalterable, scattered and permissioned nature of conducting various functions. Considering the qualities and the effectiveness of this particular technology, Emirates Islamic was the initial Islamic monetary institution (bank) of The United Arab Emirates (UAE) that adopted it for offering new cheque books to the customers as a way to strengthen cybersecurity and decrease fraudulent activities (Hassani et al., 2018). According to Riesco et al. (2020), the positive relationship amid blockchain technology and cybersecurity can be determined from a clean decentralised infrastructure, which helps to store ample data successfully and thereby prevent the occurrence of cyberattacks by a certain degree. As identified by Riesco et al. (2020), the clean decentralised infrastructure of blockchain technology possesses certain major elements that eventually generate positive or favourable results concerning the prevention of cyberattacks and fraudulent activities. These elements can be recognised as Trust, Validations, Time-Stamping, Code Transparency, Integrity, Immutable Register, Public Key Infrastructure (PKI) and Availability (Riesco et al., 2020, p.267-268).

Prior research revealed that blockchain technology tends to maintain trust under a clean decentralised infrastructure by ensuring optimum and successful execution of its available networks (Dubey et al., 2020; Meng et al., 2020). On the other hand, this specific form of technology helps to maintain and promote validations by implementing cryptographic algorithms within the mentioned accessible networks (Riesco et al., 2020). Prior reseach opined that blockchain technology is positively related to cybersecurity because it makes sure Time-Stamping of every transaction being performed within its Immutable Register, which tracks any sharing detail most efficiently (Demirkan et al., 2020; Riesco et al., 2020; Zhang et al., 2019). Code Transparency is an application under blockchain technology, which tends to preserve higher transparency level within the transactions as per the desired level (Bai & Sarkis, 2020; Riesco et al., 2020). In terms of Integrity and Availability, the research outcomes of Riesco et al. (2020) highlighted that the nodes present under this technological form run Ethereum Virtual Machines (EVM) in a way that the nodes offering Availability are operated efficiently via network incentives. Finally, concerning PKI, blockchain technology operates through wallets that help in performing various transactions timely and successfully (Riesco et al., 2020; Jiang et al., 2019).

Si et al. (2019; p.1028) observed, “The blockchain is the first distributed recording system with its own trust mechanism. It builds a reliable architecture for decentralized control through multi-node information redundancy. Blockchain technology integrates encryption, peer-to-peer transmission, consensus, distributed storage and other technologies”. These identified facets eventually support blockchain technology to form, develop as well as maintain cybersecurity in a way that any sort of transaction is being performed without facing threats (Si et al., 2019; Shaverdian, 2019; Kshetri, 2017). There are many cyberattack categories and their respective modes can be defended as well as mitigated through the help of blockchain technology along with its distinct methods (Yohan & Lo, 2020; Maroufi et al., 2019; Khan & Salah, 2018). Thus, based on the overall discussions,

Proposition 1: Blockchain Technology is positively related to Cyber Security, can be made and thereby proved to the maximum possible degree.

Blockchain Technology and Knowledge Sharing

Prior research indicated that the significance of Knowledge Management (KM) is growing extensively in this present day context as compared to the earlier years due to several crucial reasons (Antons et al., 2020; Raudeliuniene & Szarucki, 2019) A few of these reasons included the growing level of globalisation along with industrialisation, development of several innovative technologies such as blockchain and the increasing level of threats on valuable information (Chen et al., 2019; Lee, 2019). It can be argued that there is a strong as well as a direct association amid blockchain technology and KM or Knowledge Sharing (KS) (Riesco et al., 2020; Li et al., 2019). Further, blockchain technologies could be applied to the domain of KM or KS by a considerable extent (Li et al., 2019; Si et al., 2019). It is evident that “know-who”, “know-what”, “know-why” and “know-when” are regarded as some of the KM or KS products that can be related to blockchain technologies. For instance, concerning the products of "know-who" and "know-what", these technologies facilitate in recognising the actors who have generated or modified the models and providing evidence about the transparency of their contents respectively (Fill & Harer, 2018).

Prior research indicated that KS is one of the major elements of KM, wherein blockchain technologies can facilitate the same by ensuring optimum utilisation of its capabilities (Stojanović-Aleksić et al., 2019; Zhu et al., 2019). Adeleke (2019) highlighted that KS is one of the core functions of the learning organisations, which support them to make sure optimum utilisation of the available resources and thereby raise the overall productivity as well as profitability levels at large. Therefore, to form, develop, preserve and promote KS, the learning organisations tend to use blockchain technology by propelling knowledge with a new level of innovation and developing the existing infrastructural facilities among others (Adeleke, 2019). Therefore, based on this ground, the learning organisations are often identified to implement blockchain technology in a way that a sense of the greater degree of communication level could be estab-

lished amid the organisational employees and thereby sustainability for a longer period is ensured.

The essence of using blockchain technology for KS is growing extensively amid various organisations operating in any specific business market or industry in any region throughout the world (Riesco et al., 2020; Li et al., 2019). Gaining the popularity of using this specific technology for KS in distinct business corporations is mainly due to some promising characteristics associated with it (Sakho et al., 2019; Schlichter, 2018). Under this circumstance, the report highlighted that blockchain technology possesses the exclusive feature of facilitating the network users to exchange and share valuable information amid them in the most as well as secured way through its networks or nodes (Si et al., 2019; Ølnes et al., 2017). Moreover, the blockchain technology is capable enough to establish trust amid the network participants and develop a strong connection amid various participants entailing educators and creators among others, resulting into smooth KS within any organisation (Dubey et al., 2020; Montecchi et al., 2019). Therefore, based on these grounds,

Proposition 2: Blockchain Technology is positively related to Knowledge Sharing, can be made and thereby proved by a certain extent.

Blockchain Technology and Business Transaction

Blockchain technology is an effective method for conducting business transactions safely in various ways (Hartmann & Thomas, 2020; O'Leary, 2018). For instance, Bott and Milkau (2017) observed that this particular technology is identified to support the Central banks in resolving privacy issues related to their 'electronic cash' via efficient execution of "distributed ledger technology" (DLT). This 'distributed ledger' is comprised of two specific categories that entail Permissioned Distributed Ledgers (PDL) and Non-Permissioned Distributed Ledgers (NDPL) (de Meijer, 2015, p. 222). Numerous Central banks regarding their payment services, in particular, to be one of the main operational functions, blockchain technology proved to be an effective mean in maintaining the security of these functions via synchronising different network participants and developing their consensus towards distributed networks among others (Bott & Milkau, 2017). Similar findings have also been presented by Dai and Vasarhelyi (2017), wherein the two authors elucidated that blockchain technology has been acting as a successful tactic to record distinct sorts of business transactions relating to cryptocurrency since the fiscal year of 2009. As mentioned by Dai and Vasarhelyi (2017), the privacy, as well as the security of business transactions, is maintained by blockchain technology through the association of different emerging technologies that embraced IoT, Crowdsourcing, Artificial Intelligence (AI) and Robotics among others. There are varied facets of blockchain technology that eventually help to ensure the privacy of business transactions to the maximum possible extent.

Blockchain technology and its usage are not only applicable in banking transactions but also in other domains as well as embracing transport, public administration and logistics. In this

context, Koh et al. (2020) revealed that seamless mobility of products and/or services generally flow amid the cross-borders, which eventually raise a question about the safety of the business transactions being conducted therein. Thus, a paramount need of forming, developing and preserving an exclusive digital infrastructure certainly evolves to ensure successful cross-border transactions with the maintenance of utmost security as well as privacy. Moreover, Malherbe et al. (2019) stated that the business transactions are kept secured through blockchain technology because it evades third-party involvement and thereby decreases operational expenses by a certain degree. "A blockchain is a data structure that contains a chain of blocks of transactions that are linked together in sequence. The Bitcoin blockchain operates over a peer-to-peer network where the entire chain of blocks (the blockchain) is transmitted to all the nodes on the Bitcoin network" (McCallig et al., 2019, p. 54). These nature and operational facets of blockchain technology eventually make sure the safety and privacy of business transactions by an extensive level.

Liu and Zou (2018) revealed that blockchain technology is executed in "spot exchange" market based on contract law, wherein a strong association of common trust is developed amid the respective blocks. This not only increases the legitimacy of the business or the operational functions but also confirms the utmost level of safety along with privacy in "spot exchange" market at large (Liu & Zou, 2018). Besides, the financial institutions are not an exception, wherein blockchain (distributed ledger) technology plays a crucial function in maintaining the safety of their business transactions. Justifiably, O'Leary (2018) indicated that blockchain technology proves to be effective in developing business transactions by improvising the supply chain procedures in a way that sufficient level of information flows can be ensured amid the involved partners or parties. It is in this context that safety along with the privacy of business transactions concerning supply chain mechanisms lay in information accessibility and the resources available to reap numerous significant advantages (O'Leary, 2018). Neyer and Geva (2017) observed that blockchain technology acted as one of the mechanisms of maintaining privacy along with the security of business transactions by strengthening the crypto-payment mechanisms and developing cost-to-benefit ratios at large. It has been apparent that a versatile and a secured payment mode can be ensured through blockchain technology by making optimum exploitation of 'digital signature algorithms' and improvising communication infrastructures as per the desired level (Zhong et al. (2019). It is also identified that this particular technological form imposes significant impacts on auditing as well as accounting domains, which can be duly measured in the forms of continuously monitoring the business transactions and thereby preventing any sort of fraudulent activity (Wang & Kogan, 2018). Thus, after elaborating the discussed literature and arguments,

Proposition 3: Blockchain Technology is positively related to Business Transaction Privacy and Security, can be proved by a certain extent.

Conclusion

Based on the above discussion, it is thus clear that blockchain technology has a strong positive association not only with cybersecurity but also with knowledge sharing and business transaction privacy along with security. For instance, as per the obtained literature review findings and the arguments being made therein, blockchain technology is positively linked with cybersecurity due to its exclusive features of Time-Stamping, PKI, Code Transparency and Trust among others. The prominence of this specific technology could be witnessed in the banking sector, which tends to decrease the level of cyberattacks by making better use of its network platforms as well as nodes such as Bitcoins. On the other hand, blockchain technology is also viewed to get associated with KS, supporting the learning organisations, in particular, to make sure long-term sustainability under the mounting level of globalisation phase. Most importantly, as per the obtained literature review results and the arguments presented, it is evident that blockchain technology plays a critical function in addressing the issue concerning copyright infringements by transferring valuable data at a higher speed, facilitating greater access towards any valuable data on an instant basis and preserving information security. Furthermore, the acquired literature review outcomes for this research also reflected that blockchain technology has a positive linkage with business transaction privacy as well as security. This can be justified from the perspective of various business operating segments including monetary firms and transportation among others, wherein this specific technology has been able to maintain the safety of varied transactions via its distributed networks and cryptographic algorithms.

To conclude, the role and the functions of blockchain technology cannot be ignored in overcoming any kind of cyberattack, promoting KS and preserving the security of business transactions.

References

Adeleke, T. (2019). Blockchain and Learning Organizations: How the Emerging Technology Impacts Knowledge Sharing. *Dissertation*, Doctor of Management, University of Maryland University College, USA.

Angelis, J. & da Silva, E. R. (2019). Blockchain adoption: A value driver perspective. *Business Horizons, 62*, 307-314.

Antons, D., Grünwald, E., Cichy, P., & Salge, T. O. (2020). The application of text mining methods in innovation research: current state, evolution patterns, and development priorities. *R&D Management*, *50*(3), 329-351.

Bai, C., & Sarkis, J. (2020). A supply chain transparency and sustainability technology appraisal model for blockchain technology. *International Journal of Production Research*, *58*(7), 2142-2162.

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems, 19*(10), 1020-1034.

Bott, J. & Milkau, U. (2017). Central bank money and blockchain: A

payments perspective. *Journal of Payments Strategy & Systems, 11*(2), 145-155.

Chen, J., Lv, Z., & Song, H. (2019). Design of personnel big data management system based on blockchain. *Future Generation Computer Systems*, *101*, 1122-1129.

Dai, J. & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems, 31*(3), 5-21.

de Meijer, C. R. W. (2015). The UK and blockchain technology: A balanced approach. *Journal of Payments Strategy & Systems, 9*(4), 220-229.

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics, 7*(2), 189-208.

Dubey, R., Gunasekaran, A., Bryde, D. J., Dwivedi, Y. K.., & Papadopoulos, T. (2020). Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. *International Journal of Production Research*, *58*(11), 3381-3398.

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications, 126*, 45-58.

Fill, H. & Harer, F. (2018). Knowledge blockchains: Applying blockchain technologies to enterprise modeling. *Proceedings of the 51st Hawaii International Conference on System Sciences,* Hawaii, USA, 4045-4053.

Friedewald, M. & Pohoryles, R. J. (2013). Technology and privacy. *Innovation: The European Journal of Social Science Research, 26*(1-2), 1-6.

Hartmann, S., & Thomas, S. (2020). Applying Blockchain to the Australian Carbon Market. *Economic Papers*, *39*(2), p133-151.

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

Jiang, W., Li, H., Xu, G., Wen, M., Dong, G., & Lin, X. (2019). PTAS: Privacy-preserving thin-client authentication scheme in blockchain-based PKI. *Future Generation Computer Systems, 96*, 185-195.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

Koh, L., Dolgui, A., & Sarkis, J. (2020). Blockchain in transport and logistics – paradigms and transitions. *International Journal of Production Research, 58*(7), 2054-2062.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*, 1027-1038.

Lee, J. Y. (2019). A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. *Business Horizons*, *62*(6), 773-784.

Li, Z., Liu, X., Wang, W. M., Vatankhah Barenji, A., & Huang, G. Q. (2019). CKshare: secured cloud-based knowledge-sharing blockchain for injection mold redesign. *Enterprise Information Systems*, *13*(1), 1-33.

Liu, M. Z. & Zou, Z. (2018). The application of block chain technology in spot exchange. *Journal of Intelligent and Fuzzy Systems, 34*(2), 985-993.

Malherbe, L., Montalban, M., Bedu, N., & Granier, C. (2019). Cryptocurrencies and blockchain: Opportunities and limits of a new monetary regime. *International Journal of Political Economy, 48*, 127-152.

Maroufi, M., Abdolee, R., & Tazekand, B. M. (2019). On the Convergence of Blockchain and Internet of Things (IoT) Technologies. *Journal of Strategic Innovation & Sustainability*, *14*(1), 101-119.

McCallig, J., Robb, A., & Rohde, F. (2019). Establishing the representational faithfulness of financial accounting information using multiparty security, network analysis and a blockchain. *International Journal of Accounting Information Systems, 33*, 47-58.

Meng, W., Li, W., Yang, L. T., & Li, P. (2020). Enhancing challenge-based collaborative intrusion detection networks against insider attacks using blockchain. *International Journal of Information Security, 19*, 279-290.

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. *Internet of Things, 8*, 1-18.

Montecchi, M., Plangger, K., & Etter, M. (2019). It's real, trust me! Establishing supply chain provenance using blockchain. *Business Horizons*, *62*(3), 283-293.

Neyer, G. & Geva, B. (2017). Blockchain and payment systems: What are the benefits and costs? *Journal of Payments Strategy & Systems, 11*(3), 215-225.

O'Leary, D. E. (2018). Open information enterprise transactions: Business intelligence and wash and spoof transactions in blockchain and social commerce. *Intelligent Systems in Accounting Finance & Management*, *25*(3), 148-158.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, *34*(3), 355-364.

Raudeliuniene, J., & Szarucki, M. (2019). An Integrated Approach to Assessing an Organization's Knowledge Potential. *Engineering Economics*, *30*(1), 69-80.

Riesco, R., Larriva-Novo, X., & Villagra, V. A. (2020). Cybersecurity threat intelligence knowledge exchange based on blockchain. *Telecommunication Systems, 73*(2), 259-288.

Sakho, S., Jianbiao, Z., Essaf, F., & Mbyamm Kiki, M. J. (2019). Blockchain: Perspectives and issues. *Journal of Intelligent & Fuzzy Systems*, *37*(6), 8029-8052.

Schlichter, J. (2018). Where the Bodies of Knowledge Are Buried & How Blockchain Will Resurrect Them. *PM World Journal*, *7*(6), 1-5.

Sengupta, J., Ruj, S., & Das Bit, S. (2020). A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *Journal of Network & Computer Applications*, *149*, 1-20.

Si, H., Sun, C., Li, Y., Qiao, H., & Shi, L. (2019). IoT information sharing security mechanism based on blockchain technology. *Future Generation Computer Systems, 101*, 1028-1040.

Shaverdian, P. (2019). Start with Trust: Utilizing Blockchain to Resolve the Third-Party Data Breach Problem. *UCLA Law Review*, *66*(5), 1242-1288.

Stepanovic, I. (2014). Modern technology and challenges to protection of the right to privacy. *Annals FLB – Belgrade Law Review, 62*(3), 168-178.

Stojanović-Aleksić, V., Erić Nielsen, J., & Bošković, A. (2019). Organizational prerequisites for knowledge creation and sharing: empirical evidence from Serbia. *Journal of Knowledge Management*, *23*(8), 1543-1565.

Wang, Y. & Kogan, A. (2018). Designing confidentiality-preserving Blockchain-based transaction processing systems. *International Journal of Accounting Information Systems, 30*, 1-18.

Yang, C., Chen, X., & Xiang, Y. (2018). Blockchain-based publicly verifiable data deletion scheme for cloud storage. *Journal of Network and Computer Applications, 103*, 185-193.

Yang, M., Zhu, T., Liang, K., Zhou, W., & Deng, R. H. (2019). A blockchain-based location privacy-preserving crowdsensing system. *Future Generation Computer Systems*, *94*, 408-418.

Yohan, A., & Lo, N. (2020). FOTB: a secure blockchain-based firmware update framework for IoT environment. *International Journal of Information Security*, *19*(3), 257-278.

Zhang, R., & Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys*, *52*(3), 1-34.

Zhong, L., Wu, Q., Xie, J., Li, J., & Qin, B. (2019). A secure versatile light payment system based on blockchain. *Future Generation Computer Systems*, *93*, 327-337.

Zhu, L., Wu, Y., Gai, K., & Choo, K. R. (2019). Controllable and trustworthy blockchain-based cloud data management. *Future Generation Computer Systems, 91*, 527-535.