Security, Sustainability, and Legal Issues of Blockchain Technology Implementation: A Short Literature Review

Siti Fairuz Mohd Radzi[1], Mohd Sayuti Hassan[1,*], Nurul Syuhada Shaari[2]

[1] Center for Global Sustainability Studies, Universiti Sains Malaysia, 11800 Penang, Malaysia

ARTICLE INFO	ABSTRACT
	Blockchain, discreetly introduced by Satoshi Nakamoto in 2008, has become one of the top emerging technologies in 2016 and was first used in financial sector as the basis for Bitcoin, a crypto-currency which allows peer to peer money transaction with smart contracts without any third party in between which is different from other payment method such as Paypal or other methods to send money. Many bank institutions have adopted blockchain technology to mainstream day to day operation. Based on the review of related articles, there are three major concerns behind blockchain technology; security, sustainability, and legal. These issues have become a step-back for some companies and banks to adopt blockchain into their daily operations. Hence, this paper posits that more research is required in this area.

1. Introduction

Prior to the existence of blockchain, transaction data is stored and managed by a centralized and non-distributed database. The transaction system is usually controlled and managed by a third-party organization. For instance, in currency transaction, a buyer and seller would be highly relied on a bank or credit card organization as the middleman to fulfill the transaction. The intervention of middleman will slow down the process of the transaction between the buyer and seller and might cause duplication or double-spend. Blockchain is a new type of database that has been invented to solve the problem that a centralized and distributed database has created. The technology has been used by many companies and organizations especially those in internet commerce industries to reduce cost, eliminate intermediary and streamline transaction process. Blockchain is verified safe and secure by some experts because it is distributed to several participating computers, thus making it harder for attacker to steal the data. Crosby *et al.,* [1] provide an accurate analogy to illustrate the basis of blockchain technology; it is easier to steal a thing placed in an isolated place instead of being placed on a rack full of similar product. However, the structure of blockchain still woos critical arguments between researchers to how safe and secure blockchain technology is as compared to the way the data is managed in conventional way, which is by using non-decentralized database.

* *Corresponding author.*
E-mail address: sayuti@usm.my

2. The Blockchain Technology

Blockchain is a type of decentralized database structure which contains two types of data which are transaction and block, the term used to represent record. Instead of storing the records in a central database, the records are distributed via peer-to-peer network to several parties, making the sharing of information easier as compared to using centralized database. The technology is discreetly developed by a programming team or individual disguised under the name, Satoshi Nakamoto which is claimed to own approximately $100 million of bitcoin [2]. Nakamoto [9] published a paper titled Bitcoin: A Peer-to-Peer Electronic Cash System in 2008 to introduce the use of bitcoin in online transaction to make it easy for sender to make payment to receiver by eliminating intermediary, which is, the financial institution [3]. Since then, the term has emerged and experts in data management field begin to dig deeper to understand the underlying structure of blockchain and how the technology could benefit and change the way peer to peer transaction is managed in a decentralized and secure manner. One of the most popular systems that utilize blockchain technology is bitcoin [4]. Bitcoin is a crypto-currency or electronic currency that is used as an alternative to monetary system in online transaction. Users of bitcoin can make transaction without any intermediary and the bitcoin transaction will be recorded by blockchain; or simply put, a public ledger or spreadsheet [5]. The ledger will be distributed without being copied and made available to participating computer or called as miners to review and verify the transaction without going through a broker.

3. Issues in the Implementation of Blockchain Technology

Every great system has its own greatest flaws, so does blockchain. With the advent of blockchain, comes the underlying issues and challenges that blockchain may contribute to even though it is equipped with public-key cryptography. This paper compiles the security loopholes and environmental issues that may arise in the implementation of blockchain technology by several researchers and observers. Eyal and Sirer [6] argued that, even though the transaction ledger is distributed publicly, the practice would still put the blockchain technology in vulnerability concern. This statement is somewhat agreed by several other researchers which pointing out that blockchain, like any other technology, is exposed to cyber threat and attack [7,8]. The security and environmental issues and challenges are elaborated as follow:

3.1 Security Issues

Many researchers and observers pointed out that blockchain would likely be compromised by cyber-attacks in several means because the blockchain network is built based on trust. In his paper on blockchain technology, Nakamoto [9] claims that blockchain network would not face any security breaching activity so long as at least 50% of the miners in the network are honest. Attempting to attack or hack the building blocks network is nearly impossible because the attacker needs to attack the block including its precedence blocks to accomplish the attack. Thus, if an attack occurs, the attacker most probably comes from the dishonest participating computers within the network. If a miner or a group of miners manages to gain control over 51% of the hash, the system is highly exposed to the attack and this kind of attack is referred to as 51% attack [8]. The attacker who gains 51% of control is capable to manipulate the transaction as well as approve biased consensus within the network which could lead to double-spending problem; the act of spending the same bitcoin a couple of times [10]. This problem would not occur in the traditional transaction process as the

process involves the intervention of intermediaries which verify the transaction between the sender and receiver, thus double spending problem is less possible to occur. This is supported by Kiviat [11] who claims that abolishing intermediaries in the transaction would create double spending problem because there would be no one to preserve the centralized ledger and that allows electronic unit such as dollar to be spent more than once. To prevent such attack from occurring, a technique has been implemented to prevent the attack from happening which is called as proof-of-stake [10,12]. Proof-of-stake is a technique or algorithm that is used to validate the transaction in the blockchain network and ensure that a miner can only mine blocks based on how many blocks he holds. However, there are several critics on the effectiveness of proof-of-stake technique in preventing such attack from occurring. Huoy [12] claimed that all crypto-currencies have their flaws even though proof-of-stake is integrated in the blockchain network as a security defense against attacks. In his paper, he proved that a blockchain network equipped with proof-of-stake is still vulnerable to be attacked by dishonest nodes, and at the same time denied the claims made by computer science community that proof-of-stake can ensure that a blockchain network is immune to 51% attack. Other method to prevent 51% attack to the network is by implementing private blockchain.

Blockchain technology is best known for keeping the miners anonymous in the networks and that might contribute to security issue. Due to the fact that the data ownership in blockchain network is ambiguous whereby no one has control over the network, it may be difficult to trace a specific data once it is sold which may attract more fraud activities such as counterfeiting, theft, and misuse of data [7,13]. However, Yli-Huumo *et al.,* [8] claims that by making miners anonymous, it would be more secure for miners to confirm the transaction and that would also contribute to some interesting challenges. On the other hand, it is suggested that the anonymity in blockchain network may be improved by proposing a new technique; with several trade-offs, which is inspired by e-Cash technique [14].

Other than that, the reason why people who oppose blockchain technology claim that blockchain technology is not secure because of the new source code that is used to develop blockchain which might be vulnerable to cyber-attacks. According to Kuchler [15], most of crypto-currency companies have been relying heavily on new programming code that has yet been examined by experts for its flaws. This could pose a lot of threats to the crypto-currency companies in the future, thus more research should be done to examine the new code for any loopholes.

One of the most recent issues related to blockchain technology is the WannaCry outbreak which attacks individuals, companies, hospitals, and other agencies all around the world which deal with crucial data [16]. The attack works by breaking into a victim's computer system and decrypt the victim's files. In order to encrypt the affected files, the victim has to pay huge amount of bitcoin to the attacker as a ransom. Some computer technology observers claimed that these attackers prefer to use bitcoin currency as a payment of ransom because the bitcoin transaction is difficult to be traced because the information of the transaction such as the sender details is kept anonymous [16-18] and bitcoin technology is yet to be regulated, making it the first choice of payment method to be used by cyber-attackers [18]. However, although this technology allows anonymous transaction between the sender and the receiver, the transaction could still be traced somehow.

3.2 Sustainability Issues

Despite being profitable to the users, blockchain activities especially block mining activity is said to be unsustainable with regards to environment and economic sustainability as compared to using centralized database and bitcoin is regarded as one of the blockchain technologies that pollutes the nature [19]. According to a financial system sustainability expert, Jeremy McDaniels, it would be a

challenging task to ensure that bitcoin, which could deal with approximately 360,000 transactions per day, would not irritate the environment albeit the mining activity is managed in a proper manner [20,21]. One of the logical reasons why the blockchain design is energy-intensive is due to the fact that miners require powerful and faster computer machines to mine and earn the bitcoin and in order to perform transactions in the blockchain links, the machines are left turned on all day long [19,22]. On the other hand, crypto-currency community pointed that the efficiency of crypto-currency will improve along with the advancement of blockchain technology in the long run. In-depth research is highly needed to be conducted to compare the amount of energy consumed by blockchain technology and centralized database. Other than that, some researchers pointed out that proof-of-work activity in bitcoin mining is the main cause behind the problem with regard to environmental sustainability [8,23-25]. According to Bohme *et al.,* [25], miners who use proof-of-work calculations to mine bitcoin are expected to consume up to 173 megawatts of energy which is equivalent to 20% of energy required to run a nuclear power plant.

In term of economics sustainability, there is not much debate among researchers but crypto-currency observers claimed that blockchain technology would contribute to positive and negative impact to the economic sustainability. As for cryptocurrency system, it is suggested that the unpredictable change of cryptocurrency value such as Bitcoin has a potential to suffer from a major bubbles and crashes [2]. As for the blockchain technology itself, Morgan and Wyman [26] believe that blockchain technology is more cost saving as the technology could help companies to save up to 25% to 35% of company's asset to handle the currency. This is possible because of the blockchain's nature which could eliminate the third-party intervention, thus reducing the cost to be spent for manual processing. In the joint report, Morgan and Wyman [26] also list out the benefits of deploying blockchain to companies' system; data is managed efficiently, liquidity is improved, cost of data handling and brokerage is reduced which would lead to the increase of company's revenue, etc.

3.3 Legal Issues

Blockchain technology also is likely to contribute to some legal issues according to some researchers and observers. One of the main legal issues that policy makers all over the world have to face is the legal status of blockchain technology. There remains uncertainty on how to treat the network in term of legal status as there is no special entity to govern the blockchain network as the network is based on smart contracts; a self-executing contract without any contractual clauses [11,27]. Policy makers need to think a way on how to reconstruct the current legal framework so that the blockchain technology can fit in. It is suggested that this legal issue can be addressed by integrating the elements from the traditional contracts with the blockchain smart contracts [28].

Other issue that could possibly arise is that if an interruption or attack occurs to the network, there should be someone who is responsible to take charge of the situation. The community who opposes the implementation of crypto-currency technology pointed out that if all participants within the network are given the same privileges with no one to govern the network, it would be a chaotic situation if someone successfully attacks the network. The leaderless decentralized autonomous organization (DAO) was hacked in different occasion by anonymous hackers which has led to a devastating loss of approximately 18 million dollars from January 2018 to December 2020 and the activities were difficult to trace [10]. This incident has attracted a major debate among advocates and opponents of crypto-currency technology on who should hold the legal responsibilities after the attack.

Central banks in several countries have taken steps to regulate the implementation of blockchain technology within the countries. In Malaysia, the Central Bank of Malaysia has yet to implement any

specific regulations on blockchain technology at present though the new governor of central bank has voiced out his supports towards financial technology development in Malaysia. The central bank is currently issuing a discussion paper to all banks in Malaysia and financial technology providers to ask their opinion or comment with regard to financial technology development such as blockchain, in term of the consumer protection, its feasibility and its implications to financial markets before embarking official regulation on financial technology which was expected to be ready by July 2016 [29]. This is the normal practice in Malaysia where it would take a few years for a new technology to be approved in any industry in Malaysia as the technology needs to be assessed scrutinously by the expert and Malaysia government before being implemented. However, to date, there is still no official statement issued by the Central Bank of Malaysia about the outcome of the dissemination of the discussion paper. Unlike Malaysia, in Singapore, OCBC Bank has successfully completed its pilot payment transaction by incorporating blockchain technology in its banking operation which is supported by the Monetary Authority of Singapore (MAS) [30]. MAS has expressed its support to embrace financial technology implementation in Singapore but at the same time warns the public to be mindful of the underlying problem that bitcoin could possibly contribute in the long [31].

4. The Future of Blockchain Technology

Although blockchain technology faces immense challenges even from the beginning of its implementation, the technology could somehow be improved from time to time to help facilitate transaction activities. Blockchain technology has a lot to offer apart from being used to help storing asset virtually. The technology could be extended for a number of applications such as distribution of welfare, secure voting, transfer of land titles and many more [32]. A huge number of financial companies are exploring the benefit the underlying framework of blockchain technology before adopting the technology to mainstream the business operation and this number is expected to increase from time to time. Several companies, however, have incorporated blockchain technology into their business operation. Despite being bombarded with a lot of information regarding the loopholes of blockchain technology, these early adopters can have a lot of benefit for starting to discover and adopt the technology from its earliest phase. According to Kelly [33], these early adopters could predict any disruptions in the future and they are prepared for any glitches much ahead from their new competitor who is still struggling to understand the technology and the disruption that might occur. However, early adopters might face several challenges when adopting newly discovered technology such as incompetence and lack of supports if any issues occur which may lead to greater security risk [34]. Several companies in some countries have taken a 'wait and see' approach to see whether blockchain could really worth the investment or otherwise.

In Malaysia, an independent non-profit industry-government group has taken the initiative to nurture the development of blockchain industry in Malaysia though the Central Bank of Malaysia has yet to release any regulatory framework for financial technology despite it was expected to be ready by 2016. The group, the Malaysian Industry-Government Group for High Technology (MiGHT) collaborated with a blockchain advocacy body, Bloktex to develop blockchain industry in Malaysia [35]. MiGHT and Bloktek has organized a conference as the first step to introduce and increase awareness on blockchain technology to the public. The conference aimed to disseminate information regarding blockchain technology in term of what the technology could offer as well as its positive and negative impacts. Several banks in Malaysia have shown their interest and supports towards financial technology. These banks, namely CIMB, RHB, and Maybank, are currently working in partnership with financial technology companies in Malaysia to incorporate the technology in the current system.

5. Conclusion

This paper attempted to briefly outline the issues that blockchain might contribute to in term of security, sustainability and legal aspects by different experts and observers in blockchain technology. This paper also attempted to outline the future of blockchain technology. Though the technology faces immense challenges and disputes, this technology has a lot to offer to its potential users especially in mainstreaming transaction matters dealt by financial institutions especially in baking institutions. More studies should be conducted to discover more on how blockchain technology and its application can benefit a country, institution, or individual in the long run as well as how the technology could be made more secure from the way it is now to prevent intruders from attacking the chain. Moreover, similar to other technology, a dedicated study is paramount to develop an energy consumption model for blockchain technology. This is because the model will not only help the developers to come up with a solution to ensure that the technology is environmentally friendly, but it will likely help to improve the overall efficiency of the technology [36]

Acknowledgements

References

[1] Crosby, M., Pattanayak Nachiappan, P., Verma, S., Kalyanaraman, V." *Blockchain technology beyond bitcoin* (2015).
[2] Shu, Min, and Wei Zhu. "Real-time prediction of Bitcoin bubble crashes." *Physica A: Statistical Mechanics and its Applications* 548 (2020): 124477. https://doi.org/10.1016/j.physa.2020.124477
[3] Sarkodie, Samuel Asumadu, Maruf Yakubu Ahmed, and Phebe Asantewaa Owusu. "COVID-19 pandemic improves market signals of cryptocurrencies–evidence from Bitcoin, Bitcoin Cash, Ethereum, and Litecoin." *Finance Research Letters* 44 (2022): 102049. https://doi.org/10.1016/j.frl.2021.102049
[4] Natoli, Christopher, and Vincent Gramoli. "The balance attack against proof-of-work blockchains: The R3 testbed as an example." *arXiv preprint arXiv:1612.09426* (2016).
[5] Foley, Sean, Bart Frijns, Alexandre Garel, and Tai-Yong Roh. "Who buys Bitcoin? The cultural determinants of Bitcoin activity." *International Review of Financial Analysis* 84 (2022): 102385. https://doi.org/10.1016/j.irfa.2022.102385
[6] Eyal, I., and E. G. Sirer. "Majority mining is not enough: Bitcoin mining is vulnerable." *Financial Cryptography and Data Security (FC)* (2014). https://doi.org/10.1007/978-3-662-45472-5_28
[7] Gupta, Pooja, Volkan Dedeoglu, Salil S. Kanhere, and Raja Jurdak. "TrailChain: Traceability of data ownership across blockchain-enabled multiple marketplaces." *Journal of Network and Computer Applications* 203 (2022): 103389. https://doi.org/10.1016/j.jnca.2022.103389
[8] Yli-Huumo, Jesse, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. "Where is current research on blockchain technology?—a systematic review." *PloS one* 11, no. 10 (2016): e0163477. https://doi.org/10.1371/journal.pone.0163477
[9] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *Decentralized business review* (2008): 21260.
[10] Wang, Xu, Xuan Zha, Wei Ni, Ren Ping Liu, Y. Jay Guo, Xinxin Niu, and Kangfeng Zheng. "Survey on blockchain for Internet of Things." *Computer Communications* 136 (2019): 10-29. https://doi.org/10.1016/j.comcom.2019.01.006
[11] Kiviat, Trevor I. "Beyond bitcoin: Issues in regulating blockchain tranactions." *Duke LJ* 65 (2015): 569.
[12] Houy, Nicolas. "It will cost you nothing to "kill" a proof-of-stake crypto-currency." *Available at SSRN 2393940* (2014). https://doi.org/10.2139/ssrn.2393940
[13] Hughesa, Parka. "Beyond bitcoin: What blockchain and distributed ledger technologies mean for firms [EB/OL]." *Business Horizons* 62, no. 3 (2019): 278-281. https://doi.org/10.1016/j.bushor.2019.01.002
[14] Andola, Nitish, Vijay Kumar Yadav, S. Venkatesan, and Shekhar Verma. "Anonymity on blockchain based e-cash protocols—A survey." *Computer Science Review* 40 (2021): 100394. https://doi.org/10.1016/j.cosrev.2021.100394
[15] Kuchler, Hannah. "Cyber attacks raise questions about blockchain security." *Financial Times, Sept* 12 (2016).

[16] Akbanov, Maxat, Vassilios G. Vassilakis, and Michael D. Logothetis. "Ransomware detection and mitigation using software-defined networking: The case of WannaCry." *Computers & Electrical Engineering* 76 (2019): 111-121. https://doi.org/10.1016/j.compeleceng.2019.03.012

[17] Gadget 360. (2017). WannaCry Cyber Attacks: Why Do Hackers and Ransomware Attackers Ask for Bitcoins? Retrieved from https://www.gadgets360.com/internet/features/bitcoin-wanna-cry-virus-ransomware-cyber-attacks-hackers-1694156 on 25 May 2017.

[18] McGoogan, C., James Titcomb, and C. Krol. "What is WannaCry and how does ransomware work." *The Telegraph* (2017).

[19] Truby, Jon. "Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies." *Energy research & social science* 44 (2018): 399-410. https://doi.org/10.1016/j.erss.2018.06.009

[20] Malmo, Christopher. "Bitcoin is unsustainable." *Vice Motherboard* 29 (2015).

[21] Jenn, S. (2015). Can Bitcoin Mining Harm the Environment? Retrieved from http://www.newsbtc.com/2015/06/02/can-bitcoin-mining-harm-the-environment/ on 27 March 2017.

[22] Yuan, Xi, Chi-Wei Su, and Adelina Dumitrescu Peculea. "Dynamic linkage of the bitcoin market and energy consumption: An analysis across time." *Energy Strategy Reviews* 44 (2022): 100976. https://doi.org/10.1016/j.esr.2022.100976

[23] Swanson, Tim. "Bitcoins: made in China." *Bitcoin Magazine* 12 (2014).

[24] Jakobsson, M., and A. Juels. "Proofs of Work and Bread Pudding Protocols (Extended Abstract). Secure Information Networks (s. 258-272)." (1999). https://doi.org/10.1007/978-0-387-35568-9_18

[25] Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. "Bitcoin: Economics, technology, and governance." *Journal of economic Perspectives* 29, no. 2 (2015): 213-238. https://doi.org/10.1257/jep.29.2.213

[26] Morgan, J.P, and Oliver Wyman. "Unlocking Economic Advantage With Blockchain." Oliver Wyman. Accessed March 31, 2017. https://www.oliverwyman.com/our-expertise/insights/2016/jul/unlocking-economic-advantage-with-blockchain.html.

[27] Zachariadis, Markos, Garrick Hileman, and Susan V. Scott. "Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services." *Information and Organization* 29, no. 2 (2019): 105-117. https://doi.org/10.1016/j.infoandorg.2019.03.001

[28] De Graaf, T. J. "From old to new: From internet to smart contracts and from people to smart contracts." *Computer law & security review* 35, no. 5 (2019): 105322. https://doi.org/10.1016/j.clsr.2019.04.005

[29] Ng, Fintan. "BNM Governer Says Fintech Regulatory Ready by 2017." (2016).

[30] Fintechnews Singapore. "First Bank in SouthEast Asia To Use Blockchain Technology For Payment Services." *Fintechnews*, November 14, 2016. Retrieved from https://fintechnews.sg/6726/blockchain/first-bank-southeast-asia-use-blockchain-technology-payment-services/

[31] The Law Library of Congress. (2014). Regulation of Bitcoin in Selected Jurisdictions. Retrieved from https://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf on 4 April, 2017.

[32] Smith, Jamie. "There Is More to Blockchain than Moving Money. It Has the Potential to Transform Our Lives - Here's How." World Economic Forum. World Economic Forum, October 9, 2016. https://www.weforum.org/agenda/2016/11/there-is-more-to-blockchain-than-moving-money/.

[33] Kelly, Jemima. "Banks adopting blockchain'dramatically faster'than expected: IBM." *Retried on April* 10 (2016): 2018.

[34] Fernando, Yudi, Nor Hazwani Mohd Rozuar, and Fineke Mergeresa. "The blockchain-enabled technology and carbon performance: Insights from early adopters." *Technology in Society* 64 (2021): 101507. https://doi.org/10.1016/j.techsoc.2020.101507

[35] Bernama. "MiGHT, Bloktexto Jointly Develop Malaysian Blockchain Industry." *The Sun Daily*. April 10, 2017.

[36] Khairi, Danial Mohd, Mohd Azman Abas, Mohd Farid Muhamad Said, and Wan Saiful-Islam Wan Salim. "Fuel consumption mathematical models for road vehicle–A review." *Progress in Energy and Environment* 16 (2021): 59-71.