CRYPTOCURRENCY AND THE ROLE OF INDONESIAN CENTRAL BANK

Gunawan Widjaja, Krisnadwipayana University

ABSTRACT

Technology innovation played important role in human life. The creation of Bitcoin in 2008 has changed the concept of a payment system, which is currently control by the central bank. This research aims to find out what is the "possible future" role of the central bank in Indonesia in conjunction with the use of cryptocurrency as payment. The research is normative legal research. It conducted literature research through "google machine". Data collected were secondary data, which consisted of primary, secondary, and tertiary legal sources. Content analysis was conducted to reduce the collected data to become only the most relevant and reliable data. Selected data were analyzed using the qualitative method to answer the purpose of the research. The result found that the creation of Bitcoin and other cryptocurrencies reduced the role of the Central Bank. Scholars suggested that the central bank creates its cryptocurrency. Discussion suggested that many roles can be played by the central bank without creating their bitcoin. The central bank can regulate the way cryptocurrency can be used as a new way of payment. The research can be used by (Indonesian) central bank to start thinking and conducting research on how it shall regulate the use of cryptocurrency as payment. The regulations shall start on how the cryptocurrency can be created, the way cryptocurrency can be transferred, the place and process of selling and buying cryptocurrency, and the use of cryptocurrency as payment. Meanwhile, other research results were introducing on how to make the central bank's cryptocurrency; this research was the first to introduce the new role of the central bank to supervise the use of cryptocurrency as payment. The supervision that took place through the issuance of the central bank's regulations is required to avoid money laundering.

Keywords: Bitcoin, The Central Bank, Cryptocurrency, Cryptography, Indonesia.

INTRODUCTION

Technology has become more important in human life. From the first time, a computer was found, when it was used to create and store documents, technology has moved forward to become a tool of communications. Data which previously stored in a computer now can be transmitted from one computer to another anywhere. Technology can also create hardware and software that not only can make communication easy, but also to close a business transaction and subsequently making payment at the same time. The development of technology in financial activities cannot be avoided. People and corporation that involved in business shall understand and keep up with the advancement of technology in finance to support their business. Authorities shall make relevant regulations to protect businesses and laymen.

Financial technology involves many aspects of business, one among them is in the field of payment. After Nakamoto (2008) introduced Bitcoin in 2009 that can be used as a peer to peer

electronic payment, many other cryptocurrencies were then created. The creation of those cryptocurrencies was always attached to the peer to peer electronic payment. The peer-to-peer electronic payment is a payment system that would allow online payments to be sent directly from the buyer to the seller without going through a financial institution, including the central bank. There would be no authority involved in such kind of payment.

The purpose of this research is to elaborate on the legal concept of cryptography and then discuss the possibility to create and provide roles to the Indonesian central bank to supervise cryptocurrency using peer to peer electronic payment in Indonesia.

METHODS

This research is normative legal research. It conducts a literature review to obtain the necessary and required data. Literature research was conducted using "*google machine*" with keywords "*cryptography*", "*cryptocurrency*", "*bitcoin*", "*blockchain*" and "*distributed ledger technology*" combined with "*legal aspect*" and "*legal concept*". Data obtained were secondary data, which are consisted of primary legal sources, secondary legal sources, and other sources related to the subject matter. From the collected data, the researcher conducted a content analysis to find the most relevant and reliable data. Subsequently, triangulation was also conducted to verify the validity and reliability of the data by comparing the contents of the data. The remaining relevant data were then analyzed using a qualitative method with a descriptive and analytical approach to understanding the whole legal concept of cryptography. The discussion was conducted to search for the possibility to create a legal role for (Indonesian) central bank without "*directly*" involved in the creation of cryptocurrency itself.

The final data used for analysis consisted of data that provide a "*complete*" explanation of legal and technical aspects of cryptocurrency as payment. Concerning the payment, the research found that Indonesia has promulgated Law No.7 Year 2011 regarding Currency ("*Currency Law*"). Based on article 21 Currency Law and subject to relaxation on article 22 Currency Law, the only legitimate currency to be used in Indonesia is the rupiah. Any violation is subject to penal sanction as regulated in article 33 paragraph (1) Currency Law. Therefore any kind of virtual payment must also be made in Rupiah. For such purposes, the Indonesian central bank has issued Bank Indonesia (BI) Regulation No.26/6/PBI/2018 regarding Electronic Money. This regulation completed several previous regulations concerning the development and acknowledgment of the application of financial technology in Indonesia. However, those regulations are applicable for payment involving the central bank as a regulator as stipulated in Law No.23 Year 1999 regarding Bank Indonesia as amended by Law No.3 Year 2004 regarding the Amendment of Law No.23 Year 1999 regarding Bank Indonesia and Law No.6 Year 2009 regarding the Determination of Government Regulation in lieu of Law No.2 Year 2008 regarding Second Amendment Law No.23 Year 1999 regarding Bank Indonesia ("*Central Bank Law*"); and Law No.3 Year 2011 regarding Fund Transfer ("*Fund Transfer Law*"). The issuance of Fund Transfer Law was then followed by the issuance of BI Regulation No.14/23/PBI/2012 regarding Fund Transfer. None of those laws and regulations regulates cryptocurrency in Indonesia.

RESULT ANALYSIS AND DISCUSSION

The researcher found that there had been many discussions on the role of the central bank concerning cryptocurrency. Many publications made by Bank for International Settlement seemed to urge the central bank to issue its cryptocurrency. Most of them were discussing the issuance of Central Bank Digital Currencies. (Bech & Rodney, 2017; Auer, 2018; Coeuré & Jacueline, 2018; Carstens, 2018; Barontini & Henry, 2019; Lannquist, 2019). There was also discussion of the regulations of several countries concerning Cryptocurrency and its legal aspects (Law, 2018; Hughes, 2017; Hansen & Boehm, 2017; Schembri, 2018; Widjaja, 2019). However, the researcher did not find any paper discussing how shall central bank regulate cryptocurrency when the central bank, neither by becoming part of the cryptocurrency peer-to-peer transaction nor by being the creator of the Central Bank Digital Currencies.

Bitcoin represents both a virtual currency and a digital payment system (Shcherbak, 2014). World Bank (2017) referred to cryptocurrency as a digital currency. Financial Action Task Force (FATF) categorized Bitcoin as virtual currency, which can function either as a unit of account that stores a value or a medium of exchange. It must be distinct from electronic money. Electronic money is a digital representation of real money. Shcherbak (2014) added that Bitcoin can be also seen as a commodity. Hansen and Boehm (2017) treated Bitcoin as property.

Bitcoin, as introduced by Nakamoto (2008), is meant to be an alternative for cash payment, that can be paid directly from one person to another person without involving any third party as the middleman. This middleman will become the authority that would make sure that all the payment has been made and will be delivered accordingly. Bitcoin becomes digital cash with no physical form. As conducted through cryptography, whereby file data were sent directly, Bitcoin allowed money file data to be sent from buyer to the seller and directly received by the seller without the involvement of any regulator/authority that will make sure the payment will be received by the seller accordingly (Berentsen & Schär, 2018).

The security of cryptocurrency relies very much on the security of cryptography (Richards, 2018). Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables people to store data or transmit it across insecure networks so that it cannot be read by anyone in the networks except to the intended recipient (PGP Corporation, 2002). Cryptography is also known as a field of computer science and mathematics that focuses on techniques for secure communication between two parties (Alice and Bob) while a third-party (Eve and Mallory) are present (Barakat et al, 2018).

Bitcoin, as an electronic coin, is a chain of digital signatures that use cryptography (Nakamoto, 2008). In cryptography, file data can be copied and resent, meanwhile, bitcoin was never meant to copied dan resent. There will only be one transaction by using bitcoin. In a normal electronic transfer of money, there will be a financial authority that will make sure that there will be no double-spending, such as a central bank. In Bitcoin transactions, where there is no financial authority, the issuance of bitcoin and the way the payment system is conducted are organized within the Bitcoin protocol itself. The protocol will provide the rules on how the network will operate (Shcherbak, 2014). To avoid double spending in Bitcoin transactions, all transactions within the network must be made public, so that everybody in the network will only recognize one transaction. All users in the network can see the transaction by using the public key. If the transaction was modified along the way, then the private key of the modified transaction will be different. It was also if the transaction was validated by any of the users, then

the latter validation will not be count, which means that there will be no double-spending (counting) for one transaction (Nakamoto, 2008).

To make the transaction public, every transaction must be timestamped. The timestamp will include every previous timestamp in a chain. Since the timestamp is made over a block of items, it will result in a blockchain. Whenever a transaction was validated, the server will then create a new (digital) coin in the block as a proof-of-work. The new creation cannot be changed except by redoing the total block. The proof-of-work is the result of the consensus among the users in-network, which also ensures that there will be no double-spending. Each node (computer) in the network will represent one vote. This was known as a consensus mechanism, that will provide a basis for any person in the network to validate any particular transaction in the network and avoid duplication. Based on the consensus mechanism, any particular transaction can only be accepted if it is valid and has not been spent (count earlier). As the result, the acceptance will appear in the form of the creation of a new block in the blockchain (Nakamoto, 2008; Shcherbak, 2014). The Bitcoin blockchain will contain a huge data file that contains all past transactions, which may include the creation of new Bitcoin. The network user that first confirmed the transaction can get free Bitcoin. The process of confirming and getting free new Bitcoin is known as mining. The person who does the mining is called the miner. The mechanism of mining is called the consensus mechanism (Berentsen & Schär, 2018).

The legitimacy of the transaction itself is guaranteed by using a private key in asymmetric cryptography. The private key will become the signature of the encrypted money file data, even though the file data can be encrypted by everybody using the public key. The receiver of the encrypted money file data can know who has encrypted the money file data, and only the receiver can decrypt the money file data sent through the network using the private key. However, everybody in the network can get access to the new transaction information through the public key. Therefore, everybody in the network may participate to mine any Bitcoin from any transaction conducted in the network. Each information in the network which was created by a private key has a fingerprint that would allow it to be different from others. If anybody has made changes to the information, then such information would not be recognized by everybody in the network (Berentsen and Schär, 2018). It is why the approved transaction cannot be approved anymore by anybody in the network. It is only a single transaction that cannot be duplicated (Nakamoto, 2008).

The information of the transaction itself was distributed throughout the network without exception, stored, kept, and recorded in the network. The information was sent in the network in form of a block (the block candidate). Every miner that can find the valid block candidate can add the block candidate to his/her block, which made it a blockchain (Berentsen & Schär, 2018). Since all the blocks form a blockchain that looks like a ledger, it was also known as distributed ledger technology (Deshpande et al., 2017). Fanti & Viswanath (2019) stated that the bitcoin contained many layers. The first layer would be the technologies that made bitcoin available and exist as of today and in the future, that contained the consensus, storage, and computation that made it possible as a payment channel network. The payment channel networks become the second layer of bitcoin.

After Bitcoin, the market was enlivened by Altcoin, Ethereum, Ripple, NEM and Litecoin, and much more. All this was then referred to as cryptocurrencies since they all have common characteristics, i.e. decentralized and distributed. As defined by Financial Action Task Force (Financial Action Task Force, 2014), cryptocurrency is the math-based, decentralized

convertible virtual currency protected by cryptography to implement a distributed, decentralized, secure information, using public and private keys to transfer the value.

Concerning the blockchain, blockchain is not the only distributed ledger technology that has ever been known. There were many more ledger data structures that can be found. Many cryptocurrencies were also built not based on blockchain, but the other kinds of distributed ledger technology (World Bank, 2017). There were directed acyclic graphs (Bencic & Zarko, 2018) for example. Currently, there are two types of distributed ledger technology. They are the open/ permissionless distributed ledger and permissioned distributed ledger. In the open distributed ledger used by Bitcoin, there is no central owner or administrator that can select its participant in the network, everyone can enter and leave without being pre-approved. Meanwhile in a permissioned distributed ledger, to enter the network to be able to transact within the network, the intended person must be pre-approved by the owner or administrator. This main difference made open distributed ledger more transparent to the public, meanwhile the other reduced the openness. However when in the open distributed ledger, the transaction remains anonymous; in the permissioned distributed ledger the identity verification will be required before a transaction can be concluded. Bitcoin and Etherium use an open distributed ledger, meanwhile, Ripple uses a permissioned distributed ledger (World Bank, 2017).

There were at least four actors involved in the activities of cryptocurrency. They are (Shcherbak, 2014; Financial Action Task Force, 2014):

1. User, a person who uses Bitcoin or cryptocurrency to buy real or virtual goods or services and transfer payment to the seller (merchant) or who holds the virtual currency for investment only;
2. Miner, a person who takes participation in a decentralized virtual currency using his/ her computer system to validate a transaction, which upon his successful validation will obtain new virtual currency.
3. Exchanger, a person who provides on-line trading platforms to exchange virtual currency for real currency for a fee;
4. Merchant, businesses that accept virtual currency as payment for the goods and services they sold or provided.

A miner can be a user and a user can be a miner too. User can also be merchant and merchant can also play a role as a user.

Based on the description of the concept of cryptocurrency, especially Bitcoin, there were several legal issues (among others non-legal issues) that need to be attended to. They are:

Cybersecurity**:** It can be said that the security of cryptocurrencies, especially bitcoin, mimics the security of an email as they were made from and depends very much on the application of private key-public key in cryptography. Talking about cybercrime, there is always a possible threat, however, to attack an open distributed ledger with a consensus mechanism "*51% attack*" must exist. This means the attack can only succeed if the attacker can take over 51% of the network's computing power to manipulate the consensus. To avoid such kind of manipulation, the system needs to be maintained and monitored at all times (World Bank, 2017).

Governance**:** In an open distributed ledger whereby no adminitsrator will always make sure the compliance of every person in the network, there is always some person in the network that tries to change or amend the consensus. The Etherium fork and the proposal to change Bitcoin's protocol were two recent examples (World Bank, 2017).

Crash**:** Distributed ledger technology was considered as new technology, which was in the stage of development. Given the future financial transaction, some people may worry about whether distributed ledger technology can develop faster than the needs. If the distributed ledger technology cannot keep up, the possibility of a crash may happen at any time. However considering that banks, regulators, and trade associations have engaged in R3 CEV Consortium, the largest blockchain R&D consortium; and the stock exchanges around the world are testing the distributed ledger technology to be used in the stock trading platform, the apprehensive about the crash of using Bitcoin and distributed ledger technologies can be minimized.

The Anonymity of the Transaction May Lead to Money Laundering

Based on cryptography technology, all transactions of cryptocurrency are anonym. However, even though the transaction of bitcoin is anonymous, those transactions can be seen by all person the network, which made the transactions transparent. The record of every bitcoin transaction is in the publicly visible distributed ledger, every person entering the network can obtain the data of transaction made by the anonym person. The only thing they do not know is the person who did the transaction. Silk Road is one of the best examples of money laundering using peer to peer transaction that finally can be resolved (World Bank, 2017). It only needs the strong will of the authority. However not all transactions in cryptocurrency are anonym, the permissioned distributed ledger that requires the obligation for identity verification made all the transactions can be traceable.

Privacy**:** Under open distributed ledger, all transaction is anonymous which made it almost impossible for any person to know who made the transaction. On the contrary, the permission distributed ledger opens the possibility of a breach of privacy. The involvement of an administrator in every transaction will reveal the identity of the person who transact within the network and what kind of transaction is being made. For this kind of transaction, the General Data Protection Regulation (GDPR) must be implemented and enforced.

From those legal issues that need to be considered, the case of cybersecurity and crash was something that, by nature, beyond the control of the central bank. Three issues can be taken care of by the central bank, especially the Indonesian central bank. They are the issues of money laundering, governance, and data privacy.

In the case of money laundering, it can be prevented by understanding the role of the actors involved in cryptography. Because of Bitcoin and the other cryptocurrencies that used open distributed ledger, there no administrator at all. The system will manage ad regulate itself. From four actors that were known, the miner is the only actor that need not be attended to or worried about. Miner never dealt directly with the Bitcoin transaction. Miner is the actor that collects new Bitcoin using his/her expertise in algorithms and mathematics, the person who built up his/her blockchain in the system. He/she is the person that follows the consensus mechanism.

The exchanger is the person who “sells” Bitcoin to another person, which will become the user. The user will then transact with the “purchased” Bitcoin in the network and or just keep the Bitcoin for his/her investment. The most probable money laundering can take place is when the potential user buys Bitcoin from the exchanger. Under current regulation in Indonesia, trading of Bitcoin (in the physical form of coins) is regulated in BAPPEBTI Regulation No.5 Year 2019 regarding Technical Provision on the Organization of Physical Market of Crypto Asset in Futures Exchange. BAPPEBTI stands for Badan Pengawas Perdagangan Berjangka

Komiditi (Commodity Futures Trading Supervisory Board). However, there was no regulation for on-line trading of Bitcoin and other cryptocurrencies. Given the role of the exchanger is very important as the entrance for money laundering in Bitcoin or other cryptocurrencies using an open distributed ledger, there should be clear and assertive regulation for all exchangers. Know your customer (KYC) must be implemented by all exchangers. They must be responsible for any kind of transaction they made, especially when they sell Bitcoin/ cryptocurrency on-line, and subject to the application of money laundering law and regulations. User's transactions, as mentioned above can be seen publicly by monitoring the patterns of transactions through the public key. There should be rules and mechanisms that will do the monitoring and reporting on every "*suspicious"* transaction as used to be conducted by banks dan other non-bank financial institutions. The scheme used in cryptography can trace back any kind of transaction made by any user, even though it may take time, effort, and expertise. However good monitoring and reporting will be sufficient enough as a beginning on regulating cryptocurrency.

The merchant as the business that transacts with the user may keep all the required information. Merchant will receipt Bitcoin from the user. Any transaction within the network will be recorded accordingly in their block in sequential, and will never overlap with the other. So by knowing the merchant who does the transaction, the merchant can be the first to be confirmed when there was a suspicious transaction of goods or services within the network. This again requires a clear and assertive regulation for merchants, besides the monitoring and report regulations that must be done.

The monitoring and reports requirements, if combined accurately can be used to maintain good governance in a cryptocurrency transaction. At least five pillars of good corporate governance can be maintained. This will reduce the issue of governance in cryptocurrency. The central bank can follow any progress that may cause a trigger to change the governance of a certain cryptocurrency.

Concerning the breach of privacy, General Data Protection Regulation (GDPR) shall be formally made, issued, enforced, and implemented in Indonesia. The regulation shall not only cover the cryptocurrency with permissioned distributed ledger but also all transactions concerning the electronic money and real money by banks and non-bank financial institutions. This was indeed the regulation that most financial consumers needed.

Another thing that must be made into attention, especially for Bitcoin and other cryptocurrencies with no administrator is that Bitcoin and similar cryptocurrencies are not e-money. Since they are not e-money, therefore the BI Regulation No.20/6/PBI/2018 regarding Electronic Money and BI Regulation No.19/8/PBI/2017 regarding National Payment Gateway and BI Regulation No.18/40/PBI/2016 regarding Payment Transaction Processing are not applicable. Because those regulations are not applicable then the central bank (BI) shall issue further regulations to regulate cryptocurrencies in Indonesia. No regulation is not wise since the existence of such cryptocurrencies in Indonesia cannot be avoided. From the above discussion it is known that even though the type of cryptocurrency transaction is decentralized and peer to peer, it does not mean that the existence of cryptocurrency cannot be regulated. It would be much better if it can involve international coordinations to establish some kind of task force to monitor cryptocurrency transactions to avoid or even to uncover money laundering transactions.

CONCLUSION

Results and discussion conducted proved that the Indonesian central bank can create its role in monitoring cryptocurrencies, instead of creating its own Central Bank Digital Currencies. The monitoring function shall be established concurrently with the regulation to register cryptocurrencies and their activities, registration of exchangers and merchants involved in cryptocurrencies activities, the obligations to be bound by "KYC" regulations, and the obligations to report suspicious transactions. These regulations will prevent money laundering as well as to keep good governance in cryptocurrency. Besides, the issuance of the General Data Protection Regulation (GDPR) becomes compulsory.

REFERENCES

Auer, R. (2018). A primer on central banks and digital currencies. *Paper presented at Conference on "Digital Finance, market disruption, and financial stability" Banque de France and Toulouse School of Economics, Paris.*

Barakat, M., Christian, E., & Timo, H. (2018). *An introduction to cryptography*.

Barontini, C., & Henry, H. (2019). *Proceeding with caution: A survey on central bank digital currency*. BIS Papers No 101.

Bech, M., & Rodney, G. (2017). Central bank cryptocurrencies. *BIS Quarterly Review*, *20*(1), 55-70.

Bencic, F.M., & Zarko, I.P. (2018). Distributed ledger technology; Blockchain compared to directed acyclic graph. *Proceeding paper presented at IEEE 38th International Conference on Distributed Computing System (ICDCS). Viena*.

Berentsen, A., & Fabian, S. (2018). A short introduction to the world of cryptocurrencies. *Federal Reserve Bank of St. Louis Review*.

Carstens, A. (2018). *Money in the digital edge: What are role of central banks?* Lecture at House of Finance Goethe University, Frankfurt.

Coeuré, B., & Jacueline, L. (2018). *Central bank digital currencies.* Bank for International Settlement.

Deshpande, A., Katherine, S., Louise, L., & Salil, G. (2017). *Understanding the landscape of distributed ledger technologies/ blockchain: Challenges, opportunities and the prospects of standards*. Cambridge: RAND's publications.

Fanti, G., & Viswanath, p. (2019). *Decentralized payment systems: Principles and design*.

Financial Action Task Force. (2014). *FATF report: Virtual currencies-Key definitions and potential AML/CFT Risks*. Paris: FATF.

Hansen, J.D., & Boehm, J.L. (2017). *Treatment of Bitcoin under US property law*.

Hughes, S.D. (2017). *Cryptocurrency regulations and enforcement in the US.*

Lannquist, A. (2019). *Central banks and distributed ledger technology: How can central banks exploring blockchain today?* Geneva: World Economic Forum.

Law. (2018). *Library of congress*: *Report on regulation of cryptocurrency around the world.*

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.

PGP Corporation. (2002). An introduction to cryptography. US: PGP Corp.

Richards, T. (2018). *Cryptocurrencies and distributed ledger technology.* The speech was given in the Australian Business Economists Briefing. Sydney.

Schembri, T. (2018). *The legal status of cryptocurrencies in the European Union*. Term paper at the Faculty of Law University of Malta.

Shcherbak, S. (2014). How should bitcoin be regulated? *European Journal of Legal Studies*, *7*(1), 45-91.

Widjaja, G. (2019). Legality of cryptocurrency. *Advanced in Business Research International Journal*, *5*(2S), 20-29.

World Bank. (2017). *Distributed ledger technology and blockchain.* Fin Tech Note No.1. Washington: World Bank.