Journal of Central Banking Law and Institutions, Vol. 2 No. 1, 2023, pp. 25 - 54
e-ISSN: 2809-9885 – p-ISSN: 2827-7775
https://doi.org/10.21098/jcli.v1i2.15

GOING DIGITAL RUPIAH: SOME CONSIDERATIONS FROM SOVEREIGNTY AND CYBERSECURITY PERSPECTIVES

Zahrashafa Putri Mahardika,[a] Rizky Banyualam Permana,[b] Nadia Maulisa[a]

[a] Dept. of Economics & Technology Law, Faculty of Law Universitas Indonesia,
[b] Dept. of International Law, Faculty of Law Universitas Indonesia, Indonesia
e-mail: zahrashafa@ui.ac.id (corresponding author);
rizkybanyualam@ui.ac.id; nadiamaulisa.2014@gmail.com

Submitted: 01 July 2022 - Last revised: 16 January 2023 - Accepted: 31 January 2023

Abstract

Central banks worldwide are coming to terms with the bits and bytes of digital money, commonly referred to as Central Bank Digital Currency (CBDC). CBDC has been claimed to be safer, more secure, and inherently less volatile, unlike cryptocurrencies, as it is issued and regulated by central banks. The development of digital currency not only emerged in, and isolated developed countries' monetary policy but also came from the emerging markets. However, the policy and academic discussion on CBDC is clouded as only a significant minority of states have instituted it. From a regulatory point of view, the basic concept of CBDC is still significantly understudied. Among the emerging scholarship, there remains a paucity of study on the (legal) aspects of cybersecurity risk and resilience of the proposed CBDC. This paper explores the role of Bank Indonesia (BI), as the central bank, in implementing CBDC and conducts a preliminary expose associated with cybersecurity risks. This paper shows that CBDC understood as not only usage of Digital Ledger Technologies, (DLTs), but in all models of electronic payment. There are diverging models for the implementation of CBDC, some models involve multiple actors and electronic systems. However, as a currency the Central Bank would ultimately bear the liability for each transaction. Therefore, it is important for BI, as the central bank, consider cybersecurity risks associated with the implementation of CBDC. Cybersecurity risks in the financial sectors including CBDC, is the potential disruption caused by cyber-attacks, IT failures, personnel, and physical or infrastructure security risks.

Keywords: *Bank Indonesia, Central Bank Digital Currency, cyber security, cyber resilience, Distributed Ledger Technology*

I. INTRODUCTION

Central Bank Digital Currency (CBDC) is a recent phenomenon. CBDC has emerged as a part of digital structural transformation of financial systems. However, CBDC is perceived by the public as entirely different concept from existing electronic payment mechanisms, such as electronic money or decentralised cryptocurrency. The development of digital currency has not only

emerged or isolated developed countries' monetary policy. CBDC is also from emerging markets. However, the policy and academic discussion on CBDC remains clouded, as the policy is only under consideration in a significant minority of states. Notably, only a small number of central banks have already introduced efforts to introduce CDBCs in their respective jurisdictions. Some of the earliest adopters of CBDC include the e-Krona of Sweden,[1] and the e-Yuan of China (e-CNY).[2]

There is an emerging body of literature that has tried to capture CBDC as emerging policy consideration for central banks. These studies are in line with the efforts of central banks that are trying to implement CBDCs. In Indonesia for example, Bank Indonesia (BI) issued a technical working paper on CBDC in 2019.[3] Sidorenko and others analysed the legal and economic implications of CBDC and argued that one of the implications of CBDC would affect national security by strengthening it. At the same time, it also poses security risks including failure of vulnerable infrastructure.[4] Some scholars also see the promising future of mainstream CBDC implementation to tackle existing problems inherently found in traditional financial systems.[5] We observe that the basic concept of CBDC is still significantly ignored from a regulatory point-of-view. One of the promising conceptual analyses is provided by Hess.[6] It identified some regulatory framework models that could be applied in various jurisdictions. Regardless of the model, however, any proposed CBDC should consider the obligations applicable to each actor involved in a CBDC transaction.[7] Among the emerging scholarship, (legal) aspects of cybersecurity risk and resilience of the proposed CBDC as electronic system is still largely only a footnote.

This paper explores the role of BI, as the central bank of Indonesia, in implementing CBDC, and conducts a preliminary exposé of cybersecurity risks associated with the issuance and management of CBDCs. The discussion

---

1 Sveriges Riksbank, "E-Krona", accessed through https://www.riksbank.se/en-gb/payments—cash/e-krona/

2 Elijah Journay Fullerton & Peter J. Morgan, "The People's Republic of China's Digital Yuan: Its Environment, Design, and Implications," *ADBI Discussion Paper Series, No. 1306*, February 2022.

3 Bastian Muzbar Zams, et al. "Designing Central Bank Digital Currency for Indonesia: the Delphi-Analytic Network Process," Bank Indonesia Working Paper, WP/4/2019.

4 E. L. Sidorenko, S. V. Schelvelva, and A. A. Lykov, "Legal and Economic Implications of Central Bank Digital Currencies (CBDC)," in Svetlana Igorevna Ashmarina, et al, eds. *Economic Systems in the New Era: Stable Systems in an Unstable World* (Springer Nature, 2021), 500.

5 Frankin Allen, Xian Gu, Julapa Jagiani, "Fintech, Cryptocurrencies, and CBDC: Financial Structural Transformation in China," *Journal of International Money and Finance*, Vol. 124, June 2022,

6 Simon Hess, "Regulating Central Bank Digital Currencies: Towards a Conceptual Framework," Working Paper, SSRN, April 2020

7 *Ibid.*, 29.

is divided into five main parts. Following the introductory section, in the Section II, we engage in a current conceptual and policy discussion on what CBDC is and the legal framework applicable for CBDC. Subsequently, in the third section we underline BI's authority to issue and regulate CBDC. In this part we also explore applicable laws for BI given its role related to CBDC, and questions the applicability of sectoral laws such as the Electronic Information and Transactions Law and implementing regulations for BI. In the fourth section, we try to identify cybersecurity risks associated with the issuance of CBDC in the existing legal framework. Finally, in the concluding section we highlight some notable considerations for BI's implementation of CBDC regarding cybersecurity risks and liability.

II. GENERAL OVERVIEW OF CBDC

The concept of CBDC is a relatively foreign feature for national financial systems. However, as we have mentioned above, rapidly emerging literature has discussed CBDC from various perspectives. In this part, we examine the basics of CBDC as a policy proposal, its method of implementation, and the differences with existing electronic/digital methods of monetary transactions.

a. Revisiting the legal theory of money

Before we advance to the present discussion of money and currency in its digital or electronic form, it is useful to revisit the legal theories and basic notions of money. In economists' language, money is understood as "*[...] everything that is generally accepted as payment for goods and services and as repayments of debts*." Moreover, from an economic perspective, functions attached to money are, as a medium of exchange, a unit of account, a store of value, and a standard of deferred payment. Thus, this understanding of money in economics needs to be translated into a legal concept. From a legal point of view, the question about money is its validity of an instrument as payment. This question is essential to construct our understanding of CBDC, as fundamentally speaking, for centuries, money has been accepted as legal tender in every transaction. Thus, everything we claim and perceive as 'money' must have a clear legal basis.

The central tenet of money is attached to the State's function. It is widely established under the early law of nations that the inherently sovereign function of the state is to govern its own internal (economic) affairs through the issuance of money. Thus, practice over centuries has built up an idea called the 'state theory of money', posited in the 20th century by Georg Friedrich Knapp.[8] The state theory of money established the state's role in building

[8] Georg Friedrich Knapp, *State Theory of Money* (London: Macmillan & Co. Ltd., 1924).

money as a means of payment within its sovereign market. This theory is consistently analysed, reanalysed, and used alongside the concept of 'sovereign power over currency'. This theory permeates legal norms within the modern constitutions of many states. Ensconcing monetary power of states in a constitution establishes the existence of money as a form currency, which is the state's sovereign prerogative.[9] Knapp highlights the role of law whenever a state introduces a new means of payment:

> "[...] the law (1) should so describe the means of payment that it should be immediately recognisable. (2) The law should settle a name for the new unit of value and call the new means by payment by it. [...] (3) The unit of value which is to come into use is defined by its relation to the previous unit."

For Knapp, under this principle, it is solely the State's authority to determine the means of payment and denomination of the means of payment, as well as a definition of any new unit thereof.[10] In the modern concept, the State's exclusive authority to regulate its money is understood as a part of 'monetary sovereignty', covering: i) the right to create money the issuance of currency; ii) the right to conduct monetary policy; iii) the right to conduct an exchange rate policy; iv) the right to decide upon the appropriate amount of current and capital account convertibility via the imposition of exchange controls; and v) the organisation of financial regulations and supervision.[11]

On the other hand, there is a theory that rejects the predominant role of state in determining what 'money' is and for society. This camp refers to this theory as the 'societary theory of money'. This theory's origins can be traced to the writing of von Savigny as well as Nussbaum.[12] According to this camp, money "*is not a formal decision by the state, but the attitude taken by society - as expressed in the practices of commercial life - which is relevant in deciding what counts as money.*" This social theory posits that for a thing to be labelled and used as money, it must be agreed as customary. Hayek's Denationalisation of Money further advances *the modern reiteration of societary theory*.[13] In this treatise, he criticised the state theory by pointing out some deficiencies inherent in state-backed money. One of his criticisms addressed the mystical origin of 'legal tender' status of government-issued money. His ultimate argument is to propose the

---

[9] Claus D. Zimmermann, "The Concept of Monetary Sovereignty Revisited", *European Journal of International Law* 24, no.3 (2013): 797–818.

[10] Knapp, *State Theory,* 24.

[11] Zimmermann, "The Concept of Monetary", 3.

[12] *Ibid.*

[13] David H. Howard, "Denationalisation of Money: F.A. Hayek, (Institute of Economic Affairs, London, 1976)

idea of the privatisation of money. According to Hayek, the state's monopoly must be abolished as private money provisions would ameliorate monetary disturbances resulting from business cycles. In Hayek's understanding, the power to supply money attributed to sovereignty was clouded by mystery and 'sacred powers' of past empires. This, government monopoly tends to lead to government abuse, inevitably causing monetary disturbances. Hayek also highlights the practical uses of parallel currencies, trade coins, and private token money as an alternative to government's monopoly on money. For him, privately issued money is a private initiative that would create stable money that is superior to what is issued by the government.[14]

Yet another opposing theoretical legal perspective on money could shed some light on how contemporary policy debates on digital currency. It is observable that the existing formal practices adhering to and leaning towards the State theory of money. However, according to Zimmermann, although adherence to such a theory may seem out of touch with economic reality. Private money is no longer foreign to use in certain transactions. In fact, the rise of recent mainstream use of Bitcoin has challenged the status quo of state-issued money. Following ever-evolving circumstances, including changes in circumstances driven by the technology, the policymakers are trying to adapt by broadening the legal concept of money. Including by introducing CBDCs However, evolution of money towards its modern form certainly should be more about concepts than merely changing names.[15]

b. What is CBDC?

The introduction of Bitcoin by a person (or a group of persons) under the pseudonym of Satoshi Nakamoto attracted global attention. From its inception, the idea of having decentralised currency that could be used in transactions beyond the reach of government has apparently proven attractive to many. Cryptocurrency, as a private money, corresponds to Hayek's utopia. Hayek's premise led to the mainstream use of privately issued digital currency in the past years; the most famous and widely used being Bitcoin. According to Hayek's prediction, privately issued money should create more stable money, favouring market operators. However, as we can see from the recent crashes in value of Bitcoin (and other similar cryptocurrencies),[16] Hayek's prediction seems untenable. These recent crashes have proven, due to the volatility in its value, cryptocurrency is far from perfect as a means of payment.

---

[14] *Ibid.*, 35.

[15] Zimmermann, "The Concept of Monetary", 15.

[16] Alex Galey, "Bitcoin Is 'Officially on Vacation,' Dropping Closer to $21,000. Here's How Investors Should React" Time, August 19, 2022, https://time.com/nextadvisor/investing/cryptocurrency/bitcoin-crash-continues/

The creation of CBDC is an attempt by the government to bring together the best of the two worlds of private money and government-backed money. It could also be argued that the attempt by governments to create CBDC is a form of 'resistance' by government against cryptocurrency, supplanting and thereby suppressing the emergence of private currencies. The government is trying to re-establish its sovereignty as the monopolist in currency creation, opposing privately issued currencies.

CBDC, in broadly speaking, is the *'monetary value stored electronically [...] that represents a liability of central bank and can be used to make payments.'*[17] This core definition of CBDC encompasses various forms and models of implementation that CBDC would take. There is no technology requirement for how CBDC should be deployed, as it could be implemented with the existing technology. Nevertheless, this does not prohibit using more recent crypto techniques such as Distributed Ledger Technologies (DLTs). Baeriswyl pointed out four advantages that CBDC would contribute to the a state's existing financial systems: 1) provision of public legal tender; 2) improvements in payment system resilience; 3) promotion of sovereign payment systems; and 4) enhancement of monetary policy.[18] Similar to the definition pointed out above, the Bank for International Settlement (BIS) defined CBDC as *'central bank-issued digital money denominated in the national unit of account, and it represents a liability of the central bank.*' BIS classifies CBDCs into two types, "general purpose" or "'retail' and 'wholesale'" CBDC. A general-purpose CBDC is a new option available to the public, consumers, and businesses, for storing value and making payments, including credit transfers, direct debits, card payments, and e-money. A wholesale CBDC is similar to today's central bank reserves and settlement accounts in that it facilitates the settlement of large interbank payments or the provision of central bank money to settle transactions of digital tokenised financial assets in new infrastructures.[19]

Among the policy discussions, there are at least five design parameters of CBDC that have already been identified. These parameters include access, anonymity, intermediation, settlement, remuneration, and validation.[20] Access ensures the universality of CBDC application, whether certain restrictions are imposed on certain populations in holding CBDC. Anonymity speaks to whether transactions using CBDC are traceable to specific parties. Intermediation is

---

[17] Romain Baeriswyl, Samuel Reynard, Alexandre Swoboda, "Retail CBDC purposes and risk transfers to the central bank," SNB Working Papers, 19/2021

[18] *Ibid.*, 5-6.

[19] Bank for International Settlement, "Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies", BIS Papers No 125, 2022, 2.

[20] Di Lucido, Katherine, A Cross-Country Survey of General-Purpose Central Bank Digital Currencies (June 29, 2020). Available at SSRN: https://ssrn.com/abstract=3637684, ADBI, Discussion paper.

whether users' access CBDC *directly* or through some intermediary. Settlement is about the settlement method using either a centralised or decentralised infrastructure. Remuneration is about whether CBDC is remunerative, in other words, whether a bank imposes a certain rate of remuneration such as interest, based on the account holding. Finally, validation concerns whether transaction processing is valid and confirmable using a certain form of token or validation method for any account attached to the central bank or intermediary party.[21]

According to Hess, there are six general categories describing existing legal forms of money. These are, among others: 1) central bank deposits and cash; 2) bank deposits; 3) electronic money; 4) Money Market Mutual Fund Shares (MMMF); and 5) virtual currencies. Based on the above discussion, CBDC is a broad concept that covers not only DLT-utilizing digital currency but also all electronic money related to a central bank and has legal tender status. In contrast with the mainstream discourse, which focuses on implementing cryptography algorithms in CBDC, as the discussion has been trying to contrast the CBDC with its cryptocurrency equivalent, the use of DLT or any other cryptographic technique is not a prerequisite for a monetary instrument to be labelled as CBDC. However, it is important to clearly distinguish among CBDC, e-money, and virtual currencies. CBDC is a form of *money* in its digital form, which represents a fiat liability of central bank. Whereas e-money is '*primarily a liability of non-banks which is redeemable for commercial bank money and central bank money*'.[22] In short, e-money is a derivatives of commercial/central bank money and is not a fiat liability of central banks. Thus, any regulatory framework must differentiate between the two. We must also distinguish the virtual currency. Virtual currency is electronic money which does not acknowledge or fulfil the legal definition of a central bank deposit, bank deposit, e-money, or MMMF. Crypto-based currencies fall within this last category.[23]

By early 2022, around one hundred countries were exploring CBDCs. Some are still researching, some are still testing, and some have already circulated CBDCs to the public.[24] In general, central banks in emerging markets and developing economies have appeared more motivated to issue CBDCs than their counterparts in developed economies. This is considering that financial inclusion is a crucial consideration in determining CBDCs for these markets. An overwhelming majority of central banks highlight domestic payments' efficiency and security as reasons for central banks to consider implementing

[21] ADBI, 12.

[22] Hess, "Regulating Central Bank", 5.

[23] *Ibid.*,

[24] Kristalina Georgieva, "The Future of Money: Gearing up for Central Bank Digital Currency", accessed through https://www.imf.org/en/News/Articles/2022/02/09/sp020922-the-future-of-money-gearing-up-for-central-bank-digital-currency

CBDCs. The importance of monetary policy and financial stability as drivers of CBDCs is relatively low and diminishing in advanced economies.[25]

c. CBDC Regulatory model

As Hess pointed out, there are myriad CBDC's legal classifications determined by the access option provided to the end-user.[26] If the holder or the user of CBDC can exchange the funds directly with the central bank, it can be said that the mode of access is categorised as 'direct access'. Meanwhile, if a third party participates in the transaction of the user/holder to use or access its funds, then the access could be categorised as 'indirect' or 'hybrid'. This mode of access determines the liability rules and applicability of laws and regulations governing CBDC transactions. In summary, the mode of access could be summarised as follows:

Table 1.
Regulatory model

Model	Third party?	Users' access to central bank	Explanation
Direct access	No	Yes, direct	User has a claim directly to the central bank
Hybrid access through Payment System Provider	Yes	Yes, direct	User has a claim at the central bank, but funds are made available through PSP
Hybrid access through technical service provider	Yes	Yes, direct	User has a claim to the central bank, but a technical service provider (TSP) is involved to transfer and store CBDC
Indirect access through intermediaries	Yes	No, indirect	Intermediary offers services related to the digital assets, including account maintenance and payment, but not CBDC-holding
Indirect access to custodians	Yes	No, indirect	Custodian holds monetary deposits, e-money, or other digital currency

[25] Bert Van Roosebeke and Ryan Defina "Central Bank Digital Currencies: The Motivation", MPRA Paper No. 111006, Dec 2021, https://mpra.ub.uni-muenchen.de/111006/1/MPRA_paper_111006.pdf

[26] Hess, "Regulating Central Bank", 7.

From the above overview of regulatory models, at least three parties are identified as: 1) the central bank; 2) user/accountholder; 3) payment system provider; 4) technical service provider; 5) intermediaries; and 6) custodians. The actors involved determine the distribution of relative risks and liability.

d. The formation of CBDCs

Depending on how central banks circulate currency within an economy, there are two types of CBDC distribution, one-tier and two-tier systems. In a one-tier system, the issuance and distribution of digital currency is entirely under the control of the Central Bank. Even while it would allow for complete transparency of all payment-related data, financial services organisations could face a sharp decline in deposits. Account-based or token-based CBDCs are two options for the one-tier method. In a two-tier system, digital currency circulation is done by Central Bank, but the distribution to the market lies with financial institutions, most likely banks. The procedure would resemble how money is typically distributed. Additionally, banks may cross-sell consumers on financial products and token-based accounts.[27]

Many central banks are looking into how to make existing payment systems interoperable and are considering the involvement of the private sector, especially in activities that are customer facing. According to a survey, most central banks (76%) working on a retail CBDC are considering interoperability with current payment systems (s). Interoperability promotes the use of CBDCs and make it possible for the central bank and commercial bank money to co-exist (e.g., Group of Central Banks, 2020). Banks and other Payment Service Providers (PSPs) can send payments between systems when there is payment system interoperability, which eliminates the need for multiple system participation. As a result, end users can transfer funds smoothly into and out of their CBDC accounts.[28] Two examples of systems' interoperability are e-CNY of China and e-Krona of Sweden.

Given the market size of China, Electronic Reminbi or e-Chinese Yuan (e-CNY) is the world's most prominent effort to implement CBDC. The study for e-CNY implementation started in 2014, and this study led to Chinese implementation of CBDCs.[29] Chinese Working Group on R&D of e-CNY designed the currency as:

---

[27] Deloitte, "Central Bank Digital Currencies | Building Block of the Future of Value Transfer", accessed through <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-cbdc-noexp.pdf>

[28] Bank for International Settlement, 25.

[29] ADBI Discussion Paper, 9

> *the digital version of fiat currency issued by the PBOC and operated by authorised operators. It is a value-based, quasi-account-based and account-based hybrid payment instrument, with legal tender status and loosely coupled account linkage.*[30]

The People's Bank of China (PBC) previously conceived the technology and infrastructure for establishing e-CNY, by involving existing e-payment operators such as AliPay. According to Chinese officials' statements, e-CNY is the electronic version of the conventional yuan, which has legal tender status. In China, every firm or individual is obliged to accept e-CNY as a means of payment. The end goal of implementing e-CNY is not to completely supplant traditional cash payment in China, but rather e-CNY and physical yuan will co-exist. In terms of the technical aspects, e-CNY operates by utilizing crypto technology called 'centralised-permissioned Distributed Ledger Technology'. The processing, authentication, and clearance of transactions is done in distributed nodes. However, only acknowledged nodes are integrated with e-CNY ledgers.[31] According to the BIS, this hybrid system borrowed this concept from decentralised cryptocurrency (like Bitcoin) but only allowed certain networks of validated nodes to validate transactions. This hybrid approach bridges the features of private cryptocurrency and traditional government-backed money. Under this approach, the central bank still has the authority and access to cancel or revert transactions in case of error, whether the error is caused by the failure of system or other factors.

To date, however, there is no legal framework specifically regulating e-CNY in China, despite extensive studies carried out by the PBC. In 2020, to accommodate public comment, the PBC issued draft text of the *Law of the People's Bank of China*. Under this proposed amendment, CNY would be available the form of physical and digital forms. At the same time, the amendment sought to prohibit the use of digital tokens as means of payment in replacement with digital currency. It is previously estimated that the draft law would be enacted in 2021.[32] However, as of the completion of this paper,

[30] People's Bank of China, Working Group on E-CNY Research and Development, "Progress of Research & Development of E-CNY in China," available at http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf, 3.

[31] *Ibid.,* 10.

[32] B.L. Louie and M. Wang, "China's forthcoming digital currency: implications for foreign companies and financial institutions in China", *Journal of Investment Compliance* 22, no. 2 (2021): 195-200.

the new law has not been adopted.[33] Despite of slow progress in amending the PBC law, e-CNY is having been rolled out to the public in a limited manner.[34]

Sweden provides another example of a country that has extensively studied the potential of CBDC. A digital version of the Swedish currency, the e-krona, the introduction of which has deemed a priority, presents a new form of currency to modernise the monetary system in Sweden.[35] Some models considered for the technical design of e-Krona system include, among others, centralised model without intermediaries, centralised model with intermediaries, and decentralised model with intermediaries. All of these models employ DLTs as a basis for crypto technology. Due to its nature as CBDC, e-Krona would be issued, governed, and managed by Sverieges Riksbank, Sweden's central bank, to fulfil the fundamental functions of money.[36] Thus, even in decentralised model, Sverieges Riksbank, as proposed, would maintain a high degree control and involvement to avoid reputational risk should part of decentralised system fail.[37] Compared with China's efforts and progress, Sweden lags behind. As of the end of 2022, the e-Krona had not been rolled out. Riksbank had claimed that in 2022 e-Krona project would have entered pilot phase 2,[38] and it was planned that Riksbank would continue to work on research and development of e-Krona, including the technical testing.[39]

III. THE AUTHORITY OF BI TO ISSUE AND REGULATE CBDC

In the preceding section we discussed the core understanding of CBDCs, the underlying legal theories, and recent practices of e-CNY and e-Krona. The following section will build on this as it specifically relates to BI's authority to issue CBDC as Indonesia's digital currency.

---

[33] Jiang Xueqing & Zhou Lanxu, "Central bank seeks amendment to law for sharpening financial teeth," China Daily, August 5, 2022, https://www.chinadaily.com.cn/a/202208/05/WS62ec560fa310fd2b29e70628.html

[34] Arjun Kharpal, "China is pushing for broader use of its digital currency," CNBC, January, 10 2022, https://www.cnbc.com/2022/01/11/china-digital-yuan-pboc-to-expand-e-cny-use-but-challenges-remain.html.

[35] Hanna Armelius, et al. "The rationale for issuing e-krona in the digital era," Sverieges Riksbank Economic Review, 2020, https://www.riksbank.se/globalassets/media/rapporter/pov/artiklar/engelska/2020/200618/2020_2-the-rationale-for-issuing-e-krona-in-the-digital-era.pdf, 14.

[36] Gabriel Söderberg, "What is money and what type of money would an e-krona be?" *Sverieges Riksbank Economic Review* 3 (2018), 17.

[37] Hanna Armelius, et al. "E-krona design models: pros, cons and trade-offs," Sverges Riksbank Economic Review, 2020, 89.

[38] Sveriges Riksbank, E-Krona report: E-krona pilot phase 2, April, 2022, 3 accessed through https://www.riksbank.se/en-gb/payments--cash/e-krona/e-krona-reports/e-krona-pilot-phase-2/

[39] *Ibid.*

a. Bank Indonesia as Indonesia's Central Bank

The existence of BI is well-founded under Article 23D of the 1945 Constitution. This article states, "*The state shall possess a central bank, the structure, position, authorities, responsibilities, and independence of which shall be regulated by laws*."[40] BI's legal status as central bank of Indonesia was solidified and clarified by the enactment of Law Number 23 of 1999 on Bank Indonesia. Bank Indonesia is an independent state institution, which is ostensibly free from any interference by the Government and/or other parties, except for matters explicitly prescribed by the Law.[41] The primary objective of Bank Indonesia is to achieve and maintain the stability of the value of Rupiah.[42] In order to achieve this objective, Bank Indonesia shall prescribe and implement monetary policy, regulating and safeguarding the smoothness of the payment system, and regulating and supervising Banks.[43]

In carrying out its mandate on the payment system, Bank Indonesia is given authority related to currency. Under Article 23B of the 1945 Constitution, the denomination and value of the currency shall be stipulated by law.[44] Law No. 7 of 2011 on Currency ("Currency act") defines Rupiah as the legal tender issued by the Republic of Indonesia.[45] The determination and regulation of currency are vital economic tools, and it requires careful planning to offer legal protection and certainty. The currency's type and value must be determined for it to serve as a medium of exchange, a payment method, and a unit of measurement.

Central Bank (Law No. 13 of 1968 jo. Law No. 23 of 1999)

This law enshrined BI as central bank of the Republic of Indonesia. According to this law, the authority of BI is exclusive over the issuance of money in the form of paper and coins. As this legislation was introduced far before the emergence of electronic forms of money, it is obvious why the form of money set forth in the central bank law is limited to the forms of paper and coin. In a broader sense, Bank Indonesia has the task to regulate and maintain an uninterrupted payment system to achieve and maintain stability in the value of the Rupiah.[46] Pursuing that goal, Bank Indonesia is authorised to determine the type, price, characteristics of money to be issued, the material used, and the

[40] Indonesia, 1945 Constitution, Art. 23D.
[41] Indonesia, Law No. 23 of 1999 on Bank Indonesia, (hereinafter Bank Indonesia Law) Art. 4 (2).
[42] *Ibid*., Art. 7.
[43] *Ibid*., Art. 8.
[44] Indonesia, 1945 Constitution, Art. 23B.
[45] Indonesia, Law No. 7 of 2011 on Currency, (hereinafter Currency Law), Art. 2 (1).
[46] Bank Indonesia Law, Art. 8.

date when it becomes valid as a legal tender.[47] Bank Indonesia is also the only institution authorised to issue and circulate Rupiah and revoke, withdraw and destroy the currency from circulation.[48] In the digital environment, however, paper money and coinage are irrelevant. The regulation regarding electronic money also leaves a regulatory blind spot for the nature of CBDC. Bank Indonesia's authority over the payment system may become one of the strong reasons for recognizing CBDC.

Banking Laws (Law No. 7 of 1992, jo. Law No. 10 of 1998)

This regulatory framework encompasses all banking activities under the auspices of the BI and the Financial Services Authority. Although it is established that general banks do not have authority to issue currency, in particular modes of CDBC implementation, banks could act as third parties, specifically as custodians, connecting the end-user and the central bank. Banks as intermediary institutions directly serves the public, both individuals and businesses. There are fourteen commercial bank business activities, as stipulated by the law. These include, among others, collecting funds, distributing credit, and conducting other general banking activities. In addition, commercial banks can also carry out four others activities, including conducting activities in foreign exchange, capital placement, and pension funds.

When Bank Indonesia finally issues CBDC, banks could make derivatives. This New product, however, must be based on economic democracy under the precautionary principle,[49] to support the implementation of national development to increase equity, economic growth, and national stability towards increasing the welfare of the wider community.[50] For example, in payments or services that specifically use crypto-based currencies, banks can swap Rupiah with CBDC and then forward the funds to a specific party. Banks can also open CBDC savings accounts or demand deposit accounts, allowing their customers to store wealth, creating a new investment instrument, or as collateral for consumer borrowing. With the increase in CBDC-based banking products, the circulation of CBDC would be increasingly widespread through the community.

Currency Law (Law No. 7 of 2011)

According to this law, money is understood as a 'legitimate means of payment'.[51] This definition does not specify the form of money, although it

[47] *Ibid.*, Art. 19.

[48] *Ibid.*, Art. 20.

[49] Indonesia, Law No. 7 of 1992 on Banking, Art. 2.

[50] *Ibid.*, Art. 4.

[51] Currency Law, Art. 1.

also establishes that it is under the authority of BI to 'print' money. The concept used in this law is still based on the analogue format of money. The analogue-approach also is evident in Article 2 of Currency Law, where the Rupiah consists of money in the form of paper and coins. Explicitly, the Law is silent on electronic forms of money.

b. Legal framework of money in electronic or digital form

The regulatory framework governing electronic money in Indonesia is based on BI Regulation No. 20/6/PBI/2018 on Electronic Money. Electronic money as a payment instrument must meet the following requirements: 1) issued based on the value of money paid up in advance to an issuer; 2) the value of money is stored electronically in a server or a chip; and 3) the value of electronic money managed by an issuer does not constitute savings as specified in the Law on banking. Electronic money issued in Indonesia requires the use of Rupiah as its denomination. Also, for transactions using electronic money and conducted in Indonesian jurisdiction, use of the Rupiah is compulsory. The electronic provider can be a banking or a non-banking institution in the form of a limited liability company. As mentioned above, electronic money and CBDC are inherently different. Therefore, BI Regulation 20/6/PBI/2018 does not provide BI a legal basis to issue CBDC. Instead, another BI regulation has to be prescribed prior to implementation of digital Rupiah.

Regarding the use of crypto-based digital currencies, Indonesia remains cautious. BI regulation on Financial Technology (PBI 19/12/PBI/2017) and BI regulation on Payment Transaction Processing (PBI 18/40/PBI/2017), strictly prohibit the use of any kind of digital currency as a means of payment. Digital currency, under both regulations, is understood as 'virtual currency'. Regardless of the terms used, the meaning and regulatory intention are the same. One of the reasons for this is that no authority can be responsible for using the digital currency. This is, by its nature, because the decentralised system in the blockchain is characterised by the distribution of data to the parties/nodes. As the transaction is decentralised, according to this regulation's logic, there is nobody overseeing the network system used to validate the transactions. Neither party can be held responsible for consequence arising from transactions in virtual currency. Digital currency users may also not have information or knowledge about these consequences. In addition, digital currencies do not have an underlying asset that backs the price, and the trading value is highly volatile.[52]

[52] Emanuella, C. S., "Central Bank Digital Currency (CBDC) Sebagai Alat Pembayaran di Indonesia," *Jurist-Diction* Vol. 4, no. 6 (2021): 2243–2276. https://doi.org/10.20473/jd.v4i6.31845

The authority of Bank Indonesia in formulating CBDC requires explicit mention of digital Rupiah as one of the Rupiah's forms. Explicit stipulation of a digital version of money is needed to bridge the regulatory gap highlighted above. It is explicit in the Central Bank and Currency Laws that the forms of currency, as well as the authority to issue it, is limited to the form defined therein, either in coin or in paper. Neither the Central Bank Law nor Currency Law allows Rupiah in a digital form. Unlike electronic money, CBDC is not a derivative of paper and coin Rupiah, but instead digital Rupiah as a CBDCs is equivalent to the paper or coin form of Rupiah. Following this, Bank Indonesia can provide equivalent protection. In rupiah management such as planning, printing, issuing, distributing, revocation and retraction, and destruction[53] must also be adjusted to CBDC's unique characteristics, especially those related to cyber aspects. This is intended so that CBDC becomes a stand-alone form of currency and is equal to paper and coins, justifying its use as legal tender.

c. BI proposal for CBDC

In Indonesia, BI plans to implement CBDC in near future. However, technical and economic studies carried out by BI are still preliminary and limited. BI has considered adopting recent technology, to make monetary transaction and financial system more effective, resilient, and efficiently supervised by BI. [54] To this end, BI has studies technologies and policies used by other countries which have issued or considered to implement CBDC.[55] Recently, in July 2022, BI announced that it will issue a white paper to explore more about CBDC implementation in Indonesia.[56]

Due to the unavailability of the white paper, it is not officially known in what form Indonesia's digital Rupiah will take, how the design is drawn, and how the technicalities are planned. However, prior study published in BI's working paper suggest that Indonesia is considered more suitable for issuance of a cash-like CBDC model which is token-base, non-interest bearing, and general purpose CBDC. In addition to this, the working paper also suggested Indonesia to follow the Chinese e-CNY, as a second-best model, due to its

---

[53] Currency Law, Art. 11.

[54] Berry A. Harahap, et al. "Perkembangan Financial Technology terkait Central Bank Digital Currency (CBDC) terhadap Transmisi Kebijakan Moneter dan Makroekonomi," Bank Indonesia Working Paper WP/2/2017, http://publication-bi.org/repec/idn/wpaper/WP022017.pdf

[55] Solikin M. Juhro, "Central Bank Practices in the Digital Era: Salient Challenges, Lessons, and Implications," Bank Indonesia Working Paper, WP/1/2021, https://www.bi.go.id/id/bi-institute/policy-mix/Documents/CB_in_the_Digital_Era_2021.pdf

[56] Departemen Komunikasi Bank Indonesia, "Bersiap Kembangkan CBDC, Bi Segera Rilis White Paper", https://www.bi.go.id/id/publikasi/ruang-media/cerita-bi/Pages/Bersiap-Kembangkan-CBDC-BI-Segera-Rilis-White-Paper.aspx

similarity of backgrounds, purposes, and the target markets.[57] Thus, it is plausible that approximation of Indonesia's CDBC model would follow best available practices, which feature the following: 1) quasi-account based or account based without interest; 2) using DLTs with hybrid/centralised-permissioned nodes controlled by BI; and 3) presence of intermediaries between end user/currency holders and BI in the form of payment system providers and/or technical service providers. However, it is important to bear in mind that model that is proposed and adhered to by BI shall be firstly in the as-yet-unpublished white paper.

IV. CYBERSECURITY RISKS AND APPLICABLE LAWS FOR IMPLEMENTING CBDC

In the preceding section we elaborated on the BI's authority and legal basis for issuance of CBDC, as well as (an approximation) of proposed CDBC model by BI. In this part, we will highlight the cybersecurity and cyber law aspects pertaining to the issuance of digital Rupiah.

a. Applicability of the Electronic Information and Transaction Law

In Indonesia, the use of electronic system, in whatever form and technology, is governed by the regime of the Electronic Information and Transaction Law (the EIT Law). Pursuant to this law, electronic systems are defined as "sets of electronic devices and procedures that prepare, collect, process, analyse, store, display, announce, send, and/or disseminate electronic information." Therefore, every electronic system, in whatever technology form, used in the issuance and management of CBDC falls within this definition, consequently, must comply with the set of regulations established under the EIT Law. The legal basis for the operation of electronic systems in Indonesia is Law No. 11 of 2008 as amended by Law No. 19 of concerning Electronic Information and Transaction and the Government Regulation No. 71 of 2019 on Electronic System and Transaction Operation ("GR 71/2019") as well as other related ministerial regulations.

Based on Article 15 of the EIT Law, there is an obligation for Electronic System Operators (ESOs) to provide reliable and secure electronic systems and shall be responsible for the proper operation of the electronic systems. There are two distinct, broad categories of ESOs. They might fall under either public services ESOs and private services, which the EIT Law defines as "an activity or series of activities in the fulfilment of the need for services under

[57] Zams, et al. "Designing Central Bank", 24.

laws and regulations for every citizen and resident toward the goods, services, and/or the administrative provided by the public services provider". The EIT Law regime also mandates public services ESOs conduct registration. Further classification of public ESOs is determined by Article 5 Regulation of the Ministry of Communication and Information No. 36 of 2014 ("MR 36/2014"). Under this regulation, a public service ESO includes the electronic system that is regulated or monitored by government agencies or institutions, as well as privately-owned electronic systems that carry out public functions. In this case, the regulation determined that ESOs that functioned to serve the processing of online payment, financial transaction, storage of deposit of funds and its equivalent, are deemed to be public ESOs. It can be concluded that ESOs that are used for and related to the functioning of monetary system falls under public ESOs, regardless of the ownership of electronic systems, therefore regulations of public ESOs are applicable.

As mentioned above, there is no official publication on how technical aspect of BI's CBDC would function in near future. However, this paper speculates that electronic systems involved in the transaction of digital Rupiah will not be solely under the control and ownership of Bank Indonesia. As the BI working paper indicates one of the best models that could be followed by Indonesia is that governing the e-CNY. It is highly possible that intermediaries between currency holder and BI exist in each transaction. Consequently, there would be myriad electronic systems involved, including the electronic systems of the intermediaries. Thus, under the e-CNY model, there are at least three types of electronic systems involved: 1) BI's central electronic system; 2) electronic systems of each node when CBDC utilise DLT; and 3) electronic systems of intermediaries, that is, the payment system provider. It is undeniable that BI in the implementation of CBDC covered as the ESOs and all the regulation of EIT Law and its subordinate regulations would be applicable. Each type of ESO would also bear responsibility and legal liability regarding the operation of their own systems, and every ESO involved in CBDC transaction would be categorised as 'public ESOs' regardless of their ownership. However, questions remain regarding the distribution of liability and risks in operating the ESOs between the parties/ESOs involved in CBDC transaction.

For ESOs that function as part of nodes for processing the cryptographic transactions through DLT, it is plausible that BI would subscribe to hybrid-approach instead of fully decentralising the nodes, and BI might impose a certain degree of regulatory and technical oversight to mitigate the risks. Thus, operators of electronic systems as nodes of DLT would bear responsibility for the operationalising said systems. Whereas for intermediaries' electronic systems, even though the systems are operated by entities separate from BI,

there should be high degree of BI control and oversight involved in these transactions. Thus, BI should bear the ultimate responsibility for the design and implementation of CBDCs.[58] As we have identified, the greater role that BI has as the issuer of CBDC, and its greater responsibility compared to other ESOs involved, in the following part we will identify the cybersecurity risks that need to be mitigated in connection with the implementation and circulation of CBDC.

b. Currency as Critical Infrastructure

The discussion in the earlier sections highlights the issuance of the currency, which is an inherently sovereign feature of a state, as one of the fundamental state functions. Despite its electronic form, well-functioning and trustworthy digital money as means of payment needs to be maintained and treated as in the public interest, serving the greater population. [59] Arguably, every human-made object is doomed to fail from the beginning. It is the duty for every party that employs electronic systems to ensure and mitigate (as they cannot be eliminated entirely) these risks. Disruptions could eventually create a domino effect that would lead to a larger financial crisis. It is the ultimate role of the government to ensure the resiliency of the market that payment system is resilient, which the role of the government subsequently supported by the central bank to realise resilient payment system. [60] Therefore, in this part we highlight how electronic systems involved in operation of digital Rupiah must be treated as critical infrastructure.

Cyber security is defined by the International Telecommunication Union (ITU) as a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect cyber environment, organisation, and technologies that can be used to protect the cyber environment and organisation and users' assets.[61] ITU's broad definition allows each country to determine the cybersecurity policies and measures for ensuring and protecting security in its own jurisdiction according to the its needs. There are diverging policies and regulations in national and regional levels that govern cybersecurity. For instance, in a regional context, European Union based their

---

[58] Bank for International Settlements, *Central bank digital currencies: system design and interoperability* (BIS, 2021), 4.

[59] Hanna Armelius, et al. "The rationale for issuing e-krona in the digital era," Riksbank Working Paper, 2020, https://www.riksbank.se/globalassets/media/rapporter/pov/artiklar/engelska/2020/200618/2020_2-the-rationale-for-issuing-e-krona-in-the-digital-era.pdf

[60] *Ibid.,* 12.

[61] International Telecommunication Union, ITU-T X.1205 (04/2008), Series X: Data networks, open system communications and security, Telecommunication security, Overview of cybersecurity

cybersecurity policy on EU Regulation 2019/881 on the European Union Agency for Cybersecurity. Under this Regulation, cyber security is defined as the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.[62] One key aspect of cybersecurity is the protection of critical infrastructure employed in the cyber context.

Each country has different priorities in viewing their financial systems as critical infrastructure. The United States, based on The Critical Infrastructure Protection Act of 2001 (CIPA), includes financial services as one of critical infrastructure sectors, alongside chemical, commercial facilities, communications, critical manufacturing, dams, military defence bases, emergency services, energy, food and agriculture, government facilities, health and public healthcare, information technology, nuclear reactors, materials and waste, transportation systems, and water and wastewater systems. To implement CIPA, the United States issued the National Infrastructure Protection Plan (NIPP) of 2013, Partnering for Critical Infrastructure Security and Resilience in 2013. NIPP's purpose is to engage a wide range of stakeholders, such as state, local, tribal, federal, local entities, private organisations, non-profit organisations. Therefore, NIPP emphasises cooperation among these various stakeholders so that it can be implemented effectively. Specifically in the financial services sector, the United States has formulated the Financial Services Sector Specific Plan 2015 as derivative of NIPP 2013. Financial services sectors based on the plan share the same mission of enhancing cybersecurity and resilience by building solid collaborations and communities among private companies, government agencies, and international partners that aim to build mutual awareness of threats and vulnerabilities and facilitate coordination when a rapid response is needed if a significant occurs.[63] This collaboration was encouraged by two prominent institutions from the public and private sectors, namely the Financial Services Sector Coordinating Council and the Financial and Banking Information Infrastructure Committee. The strategies carried out by: implementing and maintaining structured routines for the timely and actionable sharing of information related to cybersecurity and physical threats and vulnerabilities among enterprises, across industry sectors, and between the private and government sectors; improving the risk management capabilities and security posture of companies in the financial services sector

[62] European Union, *Regulation of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act),* Regulation No. 881 (2019), Article. 2 paragraph (1).

[63] Department of Treasury dan Homeland Security, *Financial Services Sector-Specific Plan*, (Amerika Serikat: Department of Treasury dan Homeland Security, 2015), 3-4

and the service providers they rely on by encouraging the development and use of common approaches and best practices; cooperating with the domestic security, law enforcement, and intelligence community, financial regulatory authorities, other industrial sectors, and international partners to respond to and recover from significant incidents; and discussing policy and regulatory initiatives that advance infrastructure security and resilience priorities through solid coordination between government and industry.[64]

Meanwhile, the United Kingdom manages its critical national infrastructure through the Centre for the Protection of National Infrastructure. Critical National Infrastructure is defined as facilities, systems, sites, information, people, networks, and processes necessary for a country to function and upon which daily life depends. The UK has 13 national critical infrastructure sectors, chemicals, civil nuclear, communications, defence, emergency services, energy, finance, food, government, health, space, transport, and water.[65] Each sector has one or more Lead Government Department (LGD) responsible for the sector by ensuring protective security is in place for critical assets. The UK financial sectors for its cyber security and resilience are led by Her Majesty's Treasury, and its members, the Bank of England and the Financial Conduct Authority.[66] Members of the LGD(s) must conduct a critical evaluation process with purpose of giving risk owners in government a common approach to collecting and structuring data on the Critical National Infrastructure they are responsible for. At least there are five process to do: 1) map essential functions; 2) determine systems; 3) assess sector impacts; 4) identify supporting systems, relationships, and organisations; and 5) assess cross-sector impacts.[67]

Indonesia, in the early 2022, promulgated Presidential Regulation Number 82 of 2022 on Protection of Vital Information Infrastructure ("PR 82/2022"). IIV defined as electronic system that utilise information technology and/or operational technology, both independently and interdependently with other Electronic Systems to support strategic sectors, which in the event of disturbance, damage, and/or destruction of the infrastructure in question, will seriously affect the public interest, public services, defence and security, or the national economy. Indonesia IIV divided into 8 (eight) sectors, government administration, energy and mineral resources, transportation, finance, health, ICT, food, and defence.[68] On the other side, in 2014, the Ministry of

---

[64] *Ibid.*

[65] Centre for the Protection of National Infrastructure, "Critical National Infrastructure," accessed through https://www.cpni.gov.uk/critical-national-infrastructure-0

[66] UK Cabinet Office, "Public Summary of Sector Security and Resilience Plans", 2017, 16

[67] Centre for the Protection of National Infrastructure, "Critical National Infrastructure",

[68] Indonesia Presidential Regulation Number 82 of 2022 on Protection of Vital Information Infrastructure, (hereinafter PR 82/2022), Art. 4.

Defence of Republic Indonesia issued Guidance on Cyber Defence under Ministry Regulation Number 82 of 2014 ("MR 82/2014"). The Ministry of Defence of Republic Indonesia used "critical infrastructure" instead of "vital infrastructure"; and defined critical infrastructure as assets, systems, and networks, in physical or virtual form that are vital, where disturbances to them have the potential to threaten security, stability of the national economy, safety and public health or a combination of them.[69] Meanwhile, MR 82/2014 stated several critical sectors, namely: defence and security, energy, transportation, financial system, and various other public services.[70] Although Indonesia used two terminologies, both Presidential Regulation and Ministry of Défense Regulation stated that the financial system included as vital infrastructure and critical infrastructure, so it must get specific treatment to ensure the safety and resilience of the system, both electronically and physically.

In terms of financial services, state institutions that have the authority to establish whether an electronic system supporting financial services is categorised as vital information or not is financial sector regulatory and supervisory authority for the financial sector - Bank Indonesia, Otoritas Jasa Keuangan, and other related authorities.[71] Accordingly, when implementing CBDC, Bank Indonesia plays a significant role in ensuring the reliability of electronic systems as CBDC will seriously affect the public interest, public services, defence and security, and the national economy in the event of a disruption, damage, and/or destruction.[72] CBDC, with its objective of maintaining monetary and financial stability, given its characteristics and potential risks, can be included as vital infrastructure. Many cybersecurity threats haunt the implementation of CBDC, such as credential theft and system integrity. The Central Bank needs to ensure infrastructure use for CBDC will have a technical resilience. By including it as vital infrastructure, the direction of regulation and decision making related to cybersecurity risk will be more structured.

c. Possible cybersecurity risks for implementation of CBDC

Accelerated by the Covid-19 pandemic, when the financial system was going through an unprecedented digital transformation, the demand for online financial services dramatically increased. From the beginning of the Covid-19 pandemic until August 2021, 74% of financial firms experienced a rise in cybercrime, including data breaches, ransomware, phishing, fraud, and

[69] Indonesia Ministry of Defence, Regulation Number 82 of 2014 on Guidance on Cyber Defence.
[70] *Ibid.*, 1.
[71] PR 82/2022, Art. 4 paragraph 3.
[72] Ibid, Art. 4 paragraph 2.

account and money theft.[73] General cybersecurity objectives based on ITU are availability, integrity, which may include authenticity and non-repudiation, and confidentiality.[74] Indonesia Law Number 11 of 2008 and Law Number 19 of 2016 on Information and Electronic Transaction require electronic system providers to operate their systems reliably, securely, and responsibly ensuring best practices.[75]

Research conducted by IBM Security X-Force in 2022 shows that from 2015 through 2020, finance and insurance was the most targeted industry by cyber criminals globally; 70% of the attacks on the financial industry targeted banks; 16% targeted insurance companies; and 14% targeted other financial institutions.[76] Bank Indonesia itself in January 2022, sustained a ransomware attack by storage of approximately 14 GB worth of files,[77] but the attack did not impact its operations or compromise any critical data.[78] Motivation of cyberthreats varies, such as disruption, destruction, theft of corporate information, espionage, fraud, extortion, theft of personal information.[79]

Cybercrime perpetrators range from state actors, organised crime groups, insider threats, and hacktivists.[80] State actors can be nation-states or state-sponsored groups. The goals of these perpetrators are disruption, destruction, damage, theft, espionage, and/or financial gain. Different from the goals of state actors, organised crime groups, insider threats, and hacktivist goals are primarily to disrupt.[81]

With close interconnection between financial and technology in the digitalised society, an attack on financial institution or financial services could

---

[73] Threat Intelligence, "Cybersecurity in Finance: Risks and mitigation strategies", August 2021, accessed through https://www.threatintelligence.com/blog/cybersecurity-in-finance

[74] International Telecommunication Union, *ibid.,*

[75] Indonesia Law Number 11 of 2008 jo. Law Number 19 of 2016 on Information and Electronic Transaction, Art. 15 paragraph 1.

[76] IBM Security X-Force, "X-Force Threat Intelligence Index 2022", IBM Security, 2022, accessed through https://www.ibm.com/downloads/cas/ADLMYLAZ

[77] Vlad Constantinescu, Bitdefender, "Bank Indonesia confirms conti ransomware attack; stolen files leaked", accessed through https://www.bitdefender.com/blog/hotforsecurity/bank-indonesia-confirms-conti-ransomware-attack-stolen-files-leaked/

[78] Cisomag, "Bank Indonesia suffers ransomware attack, suspects conti involvement", accessed through https://cisomag.eccouncil.org/bank-indonesia-suffers-ransomware-attack-suspects-conti-involvement/

[79] Fabio Panetta, "cyber risks and the integrity of digital finance", introductory remarks at the sixth meeting of the ECRB, accessed through https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210930~e58b5eed9b.en.html

[80] *Ibid.*

[81] Tim Mauere and Arthur Nelson, The Global Cyber Threat, International Monetary Fund, 2021, accessed through https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

quickly spread the entire financial system and cause widespread disruption and loss of confidence.[82] The National Institute of Standards and Technology defines cybersecurity risks as "an effect on uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organisational operations (e.g., mission, functions, image, or reputation) and assets, individuals, other organisations, and the Nation.[83] Cyber risk to financial sectors, including CBDC, is the potential disruption caused by cyber-attacks, IT failures, personnel and physical security risks.[84] The personnel or human resource aspect is one of the most crucial parts of cyber security at the intra-organisational and macro-policy levels. Technology, as a tool, depends on how humans operate the tools.[85] Triplett argues that cybersecurity is not solely a technological issue but also a sociotechnical issue, because human factors are often the weakest link in creating a safe digital environment.[86] The earliest layer of cyber vulnerability lies in the capacity and capability of human resources, both from the internal business principals and users.[87] Physical security is an important part of deploying a multi-layered approach to cybersecurity. It is necessary to track who has access the system or devices and ensuring no one could use the device for a cyber-attack. Appropriate and effective physical security measures are needed when developing CBDC.

Furthermore, CBDC poses potential cybersecurity challenges that differ from challenges in the current digital financial system. The challenges include: 1) financial data can be more centralised; 2) Regulatory agencies have less visibility into data; 3) security hinges on the integrity of third-party validators; client key custody becomes more complicated; 4) client key custody becomes more complicated; 5) security relies on trusted hardware manufactures; 6) transaction revocation is more difficult; and 7) programmable transactions can be amplify the scope and scale of errors.[88]

---

[82] Jennifer Elliot and Nigel Jenkinson, "Cyber Risk is the New Threat to Financial Stability", accessed through https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/

[83] Kevin Stine, et.al., *National Institute of Standards and Technology Interagency or Internal Report 8286 (NISTIR 8286) Integrating Cybersecurity and Enterprise Risk Management (ERM)*, October 2022, https://doi.org/10.6028/NIST.IR.8286

[84] Public Summary of Sector Security and Resilience Plans, 16

[85] Tabisa Ncubukezi, "Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses," *Proceedings of the 17th International Conference on Information Warfare and Security*, 2022

[86] Triplett, W.J. "Addressing Human Factors in Cybersecurity Leadership". *Journal Cybersecurity and Privacy,* 5 (2022): 573-586, https://doi.org/10.3390/jcp2030029

[87] Faculty of Law Universitas Indonesia, Policy Paper on Indonesia Cyber Security and Resilience, 2022, 15.

[88] Giulia Fanti, Kari Kostiainen, "Missing Key: The Challenge of Cybersecurity and Central Bank Digital Currency", *Atlantic Council*, June 2022.

Using a decentralised ledger replicated across a distributed network has demonstrated the ability to improve availability and reduce single points of failure, while using cryptographic hashes ensures transaction record integrity. However, security incidents involving these same designs demonstrate the persistence of vulnerabilities. The security considerations for a CBDC are not substantially different from those for conventional payment systems, online banking, and other financial activities. Hansen argued that attackers would continue to use phishing attacks and malware to obtain credentials or private keys, malicious insiders will use their privileged access to steal assets, and nation-states will engage in espionage to access information or wreak havoc on another nation's critical infrastructure.[89]

Bank Indonesia, based on the authority under the Currency Law, as the central bank, has the authority to "print to distribute" Rupiah currency, so that when Bank Indonesia issues a CBDC, the issuing authority should be Bank Indonesia, not with another party. In such an implementation, the central bank can appoint intermediaries or third parties as the electronic or payment system providers. When this happens, Bank Indonesia is obligated to ensure the security and reliability of the electronic systems used in CBDC operations. Suppose we use the direct access of the CBDC model. In direct models of CBDC distribution, central banks distribute currency directly to the consumers accounts. Central bank will handling all currency distribution and managing all system and ledgers.[90] In that case, consumers will have a direct legal relationship with the central bank, so a contract will not be needed to be legally obligated.[91] When implementing this model, Indonesia first needs to amend its Currency Law, so it will eliminate the requirement of contracts between consumers and the central bank, because the law currently mandates this.

The direct model of CBDC does not always mean that the central bank is bound to own and organise its systems. Instead, it can delegate its authority to other parties or intermediary parties. This appointed third party operates its system on behalf of the central bank so that in terms of legal responsibility, consumers are only legally related to Bank Indonesia. This scheme is what happens in the analog payment system. Another model that Bank Indonesia can adopt is Hybrid access through third parties, using a licensing mechanism.[92] When implementing this model, Bank Indonesia will grant licenses to CBDC

[89] Tarik Hansen, and Katya Delak, "Security Considerations for a Central Bank Digital Currency," FEDS Notes. (Washington: Board of Governors of the Federal Reserve System, 2022).

[90] Bison Trails, Infrastructure and Design of Central Bank Digital Currencies, 23.

[91] Hess, "Regulating Central Bank", 11.

[92] *Ibid.*

operators with the provisions applied in technical regulations, such as ensuring the security of electronic systems, ensuring the reliability of the payment system used, including the criteria for legal entities for CBDC operators. Hybrid distribution models allowing third parties or intermediary parties (such as banks, or payment system operator) to offering products and carry out operational functions, while Bank Indonesia retain issuance and distribution functions.[93]

We recommend these two models as the basis for Bank Indonesia to continue to optimise its role in:[94]

1. providing a risk-free means of digital payments using central bank money;
2. mitigating the risk of non-sovereign digital currency;
3. expanding payment systems coverage and efficiency, including cross-border transactions;
4. expanding and accelerating financial inclusion;
5. providing new monetary policy instruments; and
6. facilitating the distribution of fiscal subsidies.

The integrated mechanism of CBDC, with Bank Indonesia as the core driver, will facilitate Bank Indonesia in carrying out its objectives, ensuring that CBDCs will increase financial inclusion and ensuring consumers rights on having a reliable and secure system.

V. CONCLUDING REMARKS

CDBC is an emerging monetary policy that many central banks are considering. Compared to other forms of 'digital currency', central bank-backed digital currency ensures the digital currency from the volatility of non-traditional digital currencies, such as cryptocurrency. It could be argued that favourable reception of central bank on CDBC proposal is the form of opposition of the states against the privately issued digital currency. CDBC tries to obtain as many as positive features of cryptocurrency and integrating it with the natural feature of traditional money. However, it is essential to note that CDBC does not necessitate the use of DLTs. At the most basic, CDBC encompasses all forms of electronic payment to the extent that it involves the central bank as a liability bearer for the holder of the currency. In CDBC transaction, depending on the governance, the user could interact directly with the central bank, or through intermediaries such as electronic payment system, technical service provider, intermediaries, and functions as connecting bridge between the

[93] Bison Trails, 31

[94] Bank Indonesia, "CBDC Role in Strengthening Implementation of Central Bank Mandate", accessed through https://www.bi.go.id/en/publikasi/ruang-media/news-release/Pages/sp_2417722.aspx

central bank and end-user as intermediary or custodian services. There is no single, one-size-fits-all solution in terms of CDBC proposal. It depends on the design, structure, and operation of the regulatory system in each jurisdiction.

The issuance of money, be it in electronic or analogue form, is an inherently sovereign function of the state, in line with the state theory of money. Thus, the electronic systems involved in CDBC transactions could be constructed as Vital/Critical Information Infrastructure. This approach affirmed by the regulations of several countries includes financial electronic system as a part of IIV, considering the magnitude of risks associated with the operation of the system. Cybersecurity is consistently one of the risks to financial institutions including CBDC. Two of the most factors that need special attention when developing CBDC is personnel or human resource and physical or infrastructure security risks. Thus, it is crucial to assess the cybersecurity risk and legal liability associated with the risk and the mitigation plan, when the Indonesian Rupiah, as CDBC becomes operational.

REFERENCES

Allen, Frankin, Xian Gu, and Julapa Jagiani. "Fintech, Cryptocurrencies, and CBDC: Financial Structural Transformation in China." *Journal of International Money and Finance*, Vol. 124 (June 2022)

Armelius, Hanna, et al. "E-krona design models: pros, cons and trade-offs." *Sverges Riksbank Economic Review* (2020)

Armelius, Hanna, Gabriela Guibourg, Andrew T. Levin and Gabriel Söderberg. "The rationale for issuing e-krona in the digital era." *Sverieges Riksbank Economic Review* (2020)

Baeriswyl, Romain, Samuel Reynard, and Alexandre Swoboda. "Retail CBDC purposes and risk transfers to the central bank." *Swiss National Bank Working Papers*, No. 19 (2021)

Bank for International Settlement. "Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies", *Bank for International Settlement Papers*, No. 125 (2022)

Bank for International Settlements. *Central bank digital currencies: system design and interoperability.* Bank for International Settlement (2021)

Bank Indonesia*, "CBDC Role in Strengthening Implementation of Central Bank* Mandate." Accessed Dec*ember 30, 2022. https://www.bi.go.id/en/publikasi/ruang-media/news-release/Pages/*sp_2417722.aspx.

Bank Indonesia. "Bersiap Kembangkan Cbdc, Bi Segera Rilis White Paper." Accessed December *30, 2022. https://www.bi.go.id/id/publikasi/ruang-*media/cerita-bi/Pages/Bersiap-Kembangkan-CBDC-BI-Segera-Rilis-

White-Paper.aspx.

Bison Trails. Infrastructure and Des*ign of Central* Bank Digital Currencies. (May 2021)

Centre for the *Protection of National Infrastructure. "Critical Nation*al Infrastructure.", Accessed December 30, 2*022. https://www.cpni.gov.uk/critical-national-infrastructure-0.*

*Cisomag. "B*ank Indonesia suffers ransomware attack, suspects conti involvement." Accessed December 30, 2022. https://cisomag.eccouncil.org/bank-indonesia-suffers-ransomware-attack-suspect*s-conti-involvement/*.

*Constantinescu, Vlad. "Bank Indones*ia confirms conti ransomware attack; stolen files leaked." Accessed December 30, 2022. https://www.bitdefender.com/blog/hotforsecurity/bank-indonesia-confirms-conti-ransomware-attack-stol*en-files-leaked/*.

Deloitte. Central Bank Digital Currencies - Building Block of the Future of Value Transfer. (2022)

Di Lucido, Kather*ine. "A Cross-Country Survey o*f General-Purpose Central Bank Digital Currencies", Asian Development Bank Instit*u*te Discussion Paper (June 2020*)*

*Elliot, Jennifer and Nigel Jenkinson. "Cyber Risk is the New T*hreat to Financial Stability." Accessed December 30, 2022. https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-f*inancial-stability/*.

*Emanue*lla, Claudia Saymindo. "Central Bank Dig*ital Currency (CBDC)* Sebagai Alat Pembayaran di Indonesia." Jurist-Diction, 4(6) (2021)

Faculty of Law Universitas Indonesia. Policy Paper on Indonesia Cyber Security and Resilience. (2022)

Fanti*, Giulia and Kari Kostiainen. Mi*ssing Key: The Challenge of Cybersecurity and Central Bank Digital Currency, Washington: Atlantic Council, 2022

Fullerton, Elijah Journay and Peter J. Morgan. "The People's Republic of China's Digital *Yuan: Its Environment, Design, and Implications." Asian Development B*ank Institute Discussion Paper Series, No. 1306 (February 2022)

Galey, Alex. "Bitcoin Is 'Officially on *Vacation,' Dropping Closer to $21,*000. Here's How Investors Shoul*d React." Accessed August 19, 2022. https://time.com/nextadvis*or/investing/cryptocurrency/bitcoin-crash-continues/.

Hansen,Tarik and Katya Delak. "Security Considerations for a Central Bank Digital Currency." Accessed December 30, 2022. https://www.federalreserve.*gov/econres/notes/feds-notes/security-considerations-for-a-central-bank-digital-curr*ency-20220203.html.

Harahap, Berry A., et *al. "Perkembangan Financial Technology terkait Centra*l Bank Digital Currency (CBDC) terhadap Transmisi Kebijakan Moneter *dan Makroekonomi." Bank Indonesia Workin*g Paper, No. 2 (2017)

Hess, Simon. "Regulating Central Bank Digital Currencies: Towards a Conceptual Framework." Social Science Research Netw*ork (April 2020).*

*IBM Security X-Fo*rce. "X-Force Threat Intelligence Index 2022." Accessed December 30, 2022. https://www.ibm.com/downloads/cas/*ADLMYLAZ.*

*International Telecommunication Union. "O*verview of cybersecurity." Recommendation ITU-T X.1205. Series X: Data networks, open system communications and security, (April 2008)

Juhro, Solikin M. "Centr*al Bank Practices in the Dig*ital Era: Salient Challenges, Lessons, and Implications," Bank Indonesia Working Paper, No.1 (2021).

Kharpal, Arjun. "China is pushing for broader use of its digital currency." Accessed January 10, 2022. https://www.cnbc.com/2022/01/11/china-digital-yuan-pboc-to-expand-e-cny-use-but-challenges-remain.html.

Knapp, Georg Friedrich. State Theory of Money, London: Macmillan & Co. Ltd., 1924

Kristalina Georgieva. " The Future of Money: Gearing up for Central Bank Digital Currency." Accessed December 30, 2022. https://www.imf.org/en/News/Articles/2022/02/09/sp020922-the-future-of-money-gearing-up-for-central-bank-digital-currency.

Louie, B.L. and M. Wang, "China's forthcoming digital currency: implications for foreign companies and financial institutions in China." Journal of Investment Compliance, Vol. 22 No. 2 (2021)

Mauere ,Tim and Arthur Nelson. "The Global Cyber Threat." Accessed December 30, 2022. https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm.

Panetta, Fabio. "Cyber risks and the integrity of digital finance - introductory remarks at the sixth meeting of the ECRB." Accessed December 30, 2022. https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210930~e58b5eed9b.en.html.

Sidorenko, E. L., S. V. Schelvelva, and A. A. Lykov, "Legal and Economic Implications of Central Bank Digital Currencies (CBDC)." in Svetlana Igorevna Ashmarina, et al., eds. Economic Systems in the New Era: Stable Systems in an Unstable World, Springer Nature, (2021)

Stine, Kevin et.al. Integrating Cybersecurity and Enterprise Risk Management (ERM). National Institute of Standards and Technology Interagency or Internal Report 8286 (October 2022)

Sveriges Riksbank. "E-Krona." Accessed December 30, 2022. https://www.riksbank.se/en-gb/payments--cash/e-krona.

Söderberg, Gabriel. "What is money and what type of money would an e-krona be?" Sverieges Riksbank Economic Review, 3 (2018)

Tabisa Ncubukezi, "Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses." Proceedings of the 17th International Conference on Information Warfare and Security (2022)

Threat Intelligence. "Cybersecurity in Finance: Risks and mitigation strategies." Accessed December 30, 2022. https://www.threatintelligence.com/blog/cybersecurity-in-finance.

United Kingdom's Cabinet Office. Public Summary of Sector Security and Resilience Plans (2017)

United States Department of Treasury dan Homeland Security. Financial Services Sector-Specific Plan, Department of Treasury dan Homeland Security (2015)

Van Roosebeke, Bert and Ryan Defina. "Central Bank Digital Currencies: The Motivation." Munich Personal RePEc Archive Paper, No. 111006 (December 2021)

Working Group on E-CNY Research and Development of the People's Bank of China. Progress of Research & Development of E-CNY in China. People's Bank of China (July 2021)

Xueqing, Jiang and Zhou Lanxu. "Central bank seeks amendment to law for sharpening financial teeth." Accessed August 5, 2022. https://www.chinadaily.com.cn/a/202208/05/WS62ec560fa310fd2b29e70628.html.

Zams, Bastian Muzbar et al. "Designing Central Bank Digital Currency for Indonesia: the Delphi-Analytic Network Process." Bank Indonesia Working Paper, No.4 (2019)

REGULATIONS

European Union. *Regulation of the European Parliament and of the Council* Number 881 of 2019 *on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).*

Indonesia, The 1945 Constitution of the Republic of Indonesia as amended by the First Amendment of 1999, the Second Amendment of 2000, the Third Amendment of 2001 and the Fourth Amendment of 2002

Indonesia, Law No. 23 of 1999 on Bank Indonesia

Indonesia, Law No. 7 of 2011 on Currency

Indonesia, Law No. 7 of 1992 on Banking

Indonesia. *Law Number 11 of 2008 jo. Law Number 19 of 2016 on Information and Electronic Transaction*.

Indonesia. *Presidential Regulation Number 82 of 2022 on Protection of Vital Information Infrastructure*.

Indonesia. Ministry of Defense. *Regulation Number 82 of 2014 on Guidance on Cyber Defense.*

This page is intentionally left blank