In Search of The Perfect Coin: China's Approach Towards Cryptocurrency and Its Own Central Bank Digital Currency

Xia Mian

Abstract

Ever since Bitcoin was introduced in 2008, Central Banks and regulators have watched carefully and cautiously over the development of cryptocurrencies. This development took a significant leap in 2019 when Facebook and the People's Bank of China almost simultaneously announced their Libra project and Digital Currency Electronic Payment (DCEP) respectively, instantaneously creating a rivalry. This paper anchors on China's DCEP, examines its potential benefits and risks to monetary policies, transaction security and customer protection, in comparison with conventional fiat currency and privately issued cryptocurrencies. The structural design of the DCEP is also reviewed to understand how these features guard against the issues identified. Overall, while making a few recommendations on constructing a fully prepared legal framework, this paper recognizes the DCEP as a promising step forward as it combines the security offered by blockchain and cryptography technology and the stability supported by the Central Bank.

RECENT DEVELOPMENTS

In Search of The Perfect Coin: China's Approach Towards Cryptocurrency and Its Own Central Bank Digital Currency

Xia Mian[*]

1. INTRODUCTION

Since the inception of Bitcoin in 2008,[1] technicians, economists, Central Banks and regulators around the world have kept a close and cautious watch on the development of cryptocurrency — a digital asset designed to work as a medium of exchange that relies on strong cryptography to provide security, control money creation and verify its transfer.[2] On top of their priority list are legal implications concerning cybersecurity, personal data protection, money-laundering and illegal activities, as well as macroeconomic considerations of its potential impact on the monetary system and whether it would one day replace the conventional fiat currencies. A decade later, in 2019, with the almost simultaneous introduction of the Digital Currency Electronic Payment (DCEP) designed by the People's Bank of China (PBOC) and Facebook's Libra project, and the associated rivalry between the two, these concerns once again came to the forefront of discussion. Facebook's top executive on the Libra project, David Marcus, was almost prophetic in his attempt to convince United States (US) regulators that "if the US does not push through with digital currencies such as Libra, other countries will, most likely China with its DCEP."[3]

While there are merits to the contention that a key defining characteristic of cryptocurrency is decentralization and freedom from government intervention,[4]

---

[*] Xia Mian, final year student, double degree programmes of law and economics, National University of Singapore; Research Assistant, NUS Centre for Banking and Finance Law. This article was completed under the supervision of Assistant Professor Lin Lin, and I would like to thank her for the immense support and guidance. All errors remain my responsibility.

1 Satoshi Nakamoto, "Bitcoin: A Peer to Peer Electronic Cash System" (2008) (last visited 13 July 2020), online (pdf): *bitcoin.org* < bitcoin.org/bitcoin.pdf > .

2 Andy Greenberg, "Crypto Currency" (20 April 2011) (last visited 13 July 2020), online: *Forbes* < www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html?sh = 67417ce7353e > .

3 David Pan, "Facebook's Marcus Says China Wins With Digital Renminbi if US Nixes Libra" (22 October 2019) (last visited 13 July 2020), online: *CoinDesk* < www.coindesk.com/facebooks-marcus-says-china-wins-with-digital-renminbi-if-u-s-nixes-libra > .

both the DCEP and Libra, although being centralized digital currencies, still consider themselves to be a cryptocurrency in the narrower technical sense of their strong reliance on cryptographic technology such as blockchain and distributed ledger technology (DLT) for security.[5] For the avoidance of doubt, this article categorizes the DCEP as a form of central bank digital currency (CBDC), in line with the general approach taken by Central Banks.[6] Nevertheless, this does not distract from a meaningful comparison between the DCEP and privately issued cryptocurrencies. The similarity in their underlying cryptographic technologies suggests that many of the risks present in privately issued cryptocurrencies would be valid concerns for the DCEP. Being widely recognized as a public alternative to privately issued cryptocurrencies, this article, therefore, compares the DCEP with privately issued cryptocurrencies to examine their competing impact on the effectiveness of monetary policies.

The significance of CBDC can be gleaned from the fact that while China started its research in 2014, other major economies in the world have been paying increasing attention in recent years. The Bank of Canada is actively building up its capacity to issue a CBDC and exploring the use of DLT in payment settlement via its Project Jasper.[7] Similarly, the Monetary Authority of Singapore is developing Project Ubin[8] and has a plan to cooperate closely with China in related research.[9] In 2020, the Bank of Canada, the Bank of England, the Bank of Japan, the European Central Bank, the Sveriges Riksbank and the Swiss

---

4 Jake Frankenfield, "Cryptocurrency" (last modified 5 May 2020), online: *Investopedia* < www.investopedia.com/terms/c/cryptocurrency.asp > .

5 Yao Qian, "A Systematic Framework to Understand Central Bank Digital Currency" (2018) 61:3 Sci. China Inf. Sci. at Section 3 "DFC is crypto-currency from technical perspective" [Qian Systematic Framework]; Libra Association Members, "An Introduction to Libra — White Paper", online (pdf): *George Mason University* < sls.gmu.edu/pfrt/wp-content/uploads/sites/54/2020/02/LibraWhitePaper_en_US-Rev0723.pdf > [Libra White Paper].

6 See e.g., Ben S.C. Fung & Hanna Halaburda, "Central Bank Digital Currencies: A Framework for Assessing Why and How" (2016) Bank of Canada Discussion Paper No. 2016-22, online (pdf): *Bank of Canada* < www.bankofcanada.ca/wp-content/uploads/2016/11/sdp2016-22.pdf > ; John Barrdear & Michael Kumhof, "The Macroeconomics of Central Bank Issued Digital Currencies" (2016) Bank of England Staff Working Paper No. 605, online (pdf): *Bank of England* < www.bankofengland.co.uk/-/media/boe/files/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies.pdf?la = en&hash = 341B602838707E5D6FC26884588C912A721B1DC1 > .

7 Bank of Canada, "Digital Currencies and Fintech: Projects" (last visited 13 July 2020), online: *Bank of Canada* < www.bankofcanada.ca/research/digital-currencies-and-fintech/projects/ > .

8 Monetary Authority of Singapore, "Project Ubin: Central Bank Digital Money using Distributed Ledger Technology" (20 November 2019) (last visited 13 July 2020), online: *MAS* < www.mas.gov.sg/schemes-and-initiatives/Project-Ubin > .

9 Helen Partz, "Singapore to Explore Central Bank Digital Currency with China" (19 June 2020) (last visited 13 July 2020), online: *Coin Telegraph* < cointelegraph.com/news/singapore-to-explore-central-bank-digital-currency-with-china > .

National Bank grouped together with the Bank for International Settlements (BIS) to share their research on CBDC and explore its utility for transboundary settlement.[10] In fact, a survey conducted by the BIS suggests that 80% of Central Banks in the world currently engage in CBDC research,[11] while Sweden and Uruguay have already piloted their e-Krona[12] and e-Peso[13] respectively.

Against this backdrop, it is important to find out what the DCEP is, how it differs from privately issued cryptocurrencies, what the advantages and risks it could bring and whether sufficient safeguards are in place to mitigate the risks. Accordingly, this article aims to summarize and analyze the Chinese government's categorically distinctive approaches towards privately issued cryptocurrencies and its own DCEP and offer some answers to the above questions. This article has six sections. Section 2 provides a basic definition of the DCEP, compares it with privately issued cryptocurrencies and other electronic payment methods and examines in detail the benefits as well as legal and economic risks associated with privately issued cryptocurrencies that could also raise valid concerns for the DCEP. Section 3 tracks the development of Bitcoin and Libra in exemplifying the practical implications of the risks identified earlier and the Chinese authority's negative response to privately issued cryptocurrencies. Section 4 examines the proposed structural design and implementation plan of the DCEP and how these features guard against the identified risks. Section 5 provides recommendations on constructing a more prepared legal framework in anticipation of the DCEP, and Section VI concludes.

Overall, this article suggests that while China has been extremely cautious about the challenges brought by privately issued cryptocurrencies and banned

---

[10] Bank of England, "Central Bank group to access potential cases for central bank digital currency" (21 January 2020) (last visited 13 July 2020), online (pdf): *Bank of England* <www.bankofengland.co.uk/-/media/boe/files/news/2020/january/central-bank-group-to-assess-potential-cases-for-central-bank-digital-currencies.pdf>.

[11] Christian Barontini & Henry Holden, "Proceeding with caution — a survey on central bank digital currency" (January 2019), online (pdf): *Bank for International Settlements* <www.bis.org/publ/bppdf/bispap101.pdf>; Codruta Boar, Henry Holden & Amber Wadsworth, "Impending arrival — a sequel to the survey on central bank digital currency" (January 2020), online (pdf): *Bank for International Settlements* <www.bis.org/publ/bppdf/bispap107.pdf>.

[12] Svergies Riksbank, "The Riksbank's e-krona project Report 1" (September 2017), online (pdf): *Svergies Riksbank* <www.riksbank.se/globalassets/media/rapporter/e-krona/2017/rapport_ekrona_uppdaterad_170920_eng.pdf> [Riksbank 1]; Svergies Riksbank, "The Riksbank's e-krona project Report 2" (October 2018), online (pdf): *Svergies Riksbank* <www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf>.

[13] See the IMF annual revision of the Uruguayan economy, where the IMF praised the e-peso project as successful. International Monetary Fund, "Uruguay — Staff Report for the 2018 Article IV Consultation" (19 January 2019) at 16, online (pdf): *IMF* <www.imf.org/~/media/Files/Publications/CR/2019/1URYEA2019001.ashxhttps://negocios.elpais.com.uy/finanzas/billete-digital-ayudar-uruguay-fmi.html>.

their use, it has not forgone the potential benefits to be reaped from their development. In fact, the DCEP is sufficiently well-positioned to take advantage of cryptographic technology while guarding against negative repercussions and legal implications inherent in privately issued cryptocurrencies. Going forward, it is important for the legal framework to catch up with technological progress in a forward-looking manner. It is also important for the government to be open, transparent and prompt in reporting the actual performance of the DCEP to gather public confidence in the project

2. THE DCEP, ITS DEFINITION, BENEFITS AND RISKS

(a) Differentiating the DCEP from Bitcoin, Libra and WeChat Pay

The general idea proposed by the PBOC behind its DCEP is "to issue a digital currency led by PBOC, based on cryptographic algorithm, while keeping the parallel issuance of hard currency and allowing the DCEP to form part of M0."[14] The precise nature of the DCEP is "*encrypted digital strings representing specific value*, guaranteed and issued by PBOC with its signature."[15] Similar to hard currency, the DCEP also represents the PBOC's liability against the public, and its value is supported by sovereign credit.[16]

As a preliminary point, it is important to be able to conceptually differentiate between the DCEP and privately issued cryptocurrencies such as Bitcoin and Libra, as well as other popular electronic means of payment such as WeChat Pay and Alipay. The money tree conceptualized by the International Monetary Fund (IMF) suggests a good categorization.[17] The IMF suggested four key attributes of *type, value, backstop* and *technology*.[18] Firstly, a *type* of money is *object-based* if a certain transaction is completed once the object (e.g., cash) changes hand. A *claim-based* payment requires a transfer of a claim on value existing elsewhere (e.g., swiping one's debit card transfers one's claim against the bank to the merchant). Secondly, the attribute of *value* asks whether the redemption of the claim in currency is at *fixed value* (e.g., the money in one's WeChat wallet has a fixed redemption value of 1:1 with the Renminbi (RMB)) or *variable value* (e.g., Libra as backed by the value of its reserve of assets). Thirdly, we are interested in whether the redemption guarantee is *backstopped* by the government or reliable

---

[14] Yao Qian, "Zhōngguó fādìng shùzì huòbì yuánxíng gòuxiǎng" [Conceptual Prototype of Chinese Digital Fiat Currency] (2016) 17 China Finance at 13-15 [Qian Conceptual Prototype]. "M0" refers to the part of money supply comprising of coins and notes that are in circulation and other money equivalent that can be easily converted to cash.

[15] *Ibid.*

[16] Qian Systematic Framework, *supra* note 5.

[17] Tobias Adrian & Tommaso Mancini Griffoli, "The Rise of Digital Money" (2019) FinTech Note No. 19/01, online (pdf): *IMF* < www.imf.org/-/media/Files/Publications/FTN063/2019/English/FTNEA2019001.ashx > . See the money tree at 3.

[18] *Ibid.*

private business entities such as Alibaba or Facebook. Lastly, the attribute of *technology* differentiates whether the settlement needs to rely on a central proprietary server for verification (e.g., transactions using Debit Cards and the DCEP are centralized, whereas Bitcoin is a primary example of a decentralized payment system).

According to these four features, the IMF categorizes the DCEP as an *object-based*, *fixed value*, *government-backed centralized currency*. The first attribute of object-based money already sets the DCEP apart from WeChat Pay, AliPay and Debit Cards, as only the DCEP has an intrinsic value similar to hard currency. In contrast, Bitcoin is recognized as object-based, variable-value, private decentralized currency, and Libra is claim-based, variable-value, private centralized currency. While the DCEP is conceptually distinct from Bitcoin and Libra, a meaningful comparison can still be made between them given that they face similar legal and economic risks.

(b) Advantages of the DCEP

The DCEP possesses unique advantages in comparison with conventional fiat currency as well as privately issued cryptocurrencies. Some of the key advantages include 1) improved efficiency of monetary policy, 2) lowered transaction cost and 3) recognition as legal tender, out of which improved monetary policy is of the greatest significance.

(i) Improved Efficiency of Monetary Policies

First and most importantly, the introduction of the DCEP would improve the efficiency of monetary policy in a few significant ways: a) the use of big data analysis would allow the PBOC to identify and mitigate uncertainty and delay caused by intermediaries such as commercial banks and consumers in the operation of monetary policies; b) the use of "forward contingents" would make sure ear-marked funds reach the intended recipients in pre-defined social-economic groups, geographical regions or industrial sectors and c) the "zero lower bound" problem could be resolved. Such benefits are over and beyond the obvious advantage of having a viable public alternative to using privately issued cryptocurrencies such as Libra and Bitcoin and thereby preventing the dilution of the monetary policy caused by two competing currencies in an economy.[19]

A. Identifying and Mitigating Uncertainty and Delay Caused by Intermediaries

Conventionally, counter-cyclical monetary policies aim to achieve their intended impact through a ripple down effect across multiple levels of intermediaries and therefore suffer from uncertainty and delay when intermediaries such as commercial banks or consumers do not behave as predicted.[20] Take open market operation (OMO) as an example: when the

---

[19] Louis Abraham & Dominique Guegan, "The Other Side of the Coin: Risks of the Libra Blockchain" (2019) University Ca' Foscari of Venice Dept. of Economics Working Paper No. 30/WP/2019, online (pdf): *SSRN* < ssrn.com/abstract = 3474237 > .

Central Bank practices OMO as a form of expansionary policy to fight recession, it first buys back government bonds from commercial banks and provides them with money in exchange. The banks can then lend the money (minus the stipulated portion of reserves) out to the general public. Thereafter, the money supply is increased through the multiplier effect when consumers who received money through transactions re-deposit them into the banks, allowing them to be loaned out again. An increase in the money supply lowers short-term interest rates and boosts consumption and other economic activities.

However, this theoretical process could be interrupted at many junctions by unpredictable behaviours of the intermediaries.[21] For instance, the chain is broken if the banks do not lend the money out, or when consumers do not re-deposit their money into the banks, or when consumers prefer to save their money and refuse to consume more even though the interest rate has been lowered. Such interruptions present a remarkable challenge to contemporary monetary policies since it is both difficult to identify which part went wrong and even harder to mitigate these outliers with precision.

The DCEP could potentially mitigate these interruptions caused by intermediaries. With the help of the Big Data Analysis Centre,[22] the PBOC can analyze the transaction history of the DCEP and efficiently pinpoint which part of the money supply in the above-mentioned process does not flow as intended, and the exact identities of intermediaries who are behaving out of sync. The PBOC can then finetune its monetary policies to deal with these abnormalities by, for example, buying more bonds from commercial banks that are more likely to loan the money out to consumers. Local governments in regions where consumers have a stronger saving mentality could also introduce incentives to boost consumption and transactions. By patching up these loopholes, the efficiency of monetary policies could be improved. Although it is acknowledged that the PBOC could already have some of such information from reports filed by commercial banks and local governments, the value-add of the DCEP is that it tremendously shortens the timeframe and therefore enables more rapid response. Furthermore, for the first time, the currency itself contains full information of its entire lifecycle, from creation, distribution, circulation to destruction. This change enables the PBOC to analyze the effectiveness of its monetary policies from start to end, eliminating existing blind spots and streamlining the process.

B. Ensuring Ear-marked Funds Reach Intended Destinations

Another major issue plaguing monetary policies in China is that funds intended for poverty alleviation and disaster relief are sometimes embezzled by

---

[20] Andrew B. Abel, Ben S. Bernanke & Dean Croushore, *Macroeconomics*, 8th ed. (US: Pearson, 2014), Chapter 14, "Monetary Policy and the Federal Reserve System".

[21] *Ibid.*

[22] Qian Conceptual Prototype, *supra* note 14.

corrupt local officials and never reach the hands of the poor households.[23] Some officials even falsify the headcounts of poor households and fabricate poverty reduction projects to lay claims on the funds.[24] Similarly, sector or industry-specific funds, such as funds targeted at promoting sustainable energy and environmental protection, have also been misappropriated.[25]

Misappropriation of ear-marked funds is often hard to detect in the era of hard currency, as these funds are effectively untraceable and undifferentiable once distributed. However, the DCEP shows great promise in mitigating this issue. Preliminarily, digital information carried by the DCEP allows for real-time monitoring of the flow and final destination of the funds. A red flag is immediately raised if such funds end up in the personal accounts of local officials. At a more advanced stage, the PBOC has proposed to achieve a finetuned money supply towards a certain group or sector through the use of "forward contingents."[26] The "forward contingents" can be understood as a coded set of condition precedents limiting the transfer of the DCEP. For instance, the "sector contingent" limits the sectors and entities that the ear-marked DCEP can flow into, thereby facilitating structural monetary policy and pre-empting misappropriation. "Time contingent" makes sure the transfer is only valid upon the occurrence of a specific event, such as independent verification of the identity of the recipient. Effectively, the government could require all future allocation of ear-marked funds to be implemented via the DCEP, only with "forward contingents" put in place to mitigate long-lasting issues such as inefficiencies in policy communication, potential misuse and embezzlement. This approach would also greatly enhance other major policy objectives such as poverty alleviation, closing income inequality, financing Small and Medium Enterprises (SMEs) and environmental protection, by ensuring the intended stakeholders truly receive the ear-marked funds and subsidies. At the same time, the spread of corruption can be curbed.

---

[23] See for example a Xinhua News report on 19 September 2020, criticizing a village official in Yunnan province for depositing 3.7 million RMB government funds into his own account and lost 0.2 million RMB in gambling. Xinhua, "Tā bǎ fúpín kuǎn dǎng dǔzī" [He uses poverty alleviation funds for gambling] (19 September 2020) (last visited 10 November 2020), online: *Xinhua* < www.xinhuanet.com/legal/2020-09/19/c_1126513244.htm > .

[24] Liaoning Daily, "Shěng jìwěi jiànwěi tōngbào wǔ qǐ fúpín lǐngyù fǔbài hé zuòfēng wèntí diǎnxíng ànlì" [Provincial Commission of Discipline Inspection reports five typical cases of corruption and misbehaviour in poverty alleviation] (25 September 2020) (last visited 10 November 2020), online: *Liaoning Daily* < liaoning.nen.com.cn/system/2020/09/25/021057057.shtml > .

[25] Sina, "Guǎngdōng shěng shěnjì fāxiàn chāo 2 yì yuán shuǐlì zhuānxiàng zījīn bèi jīzhàn nuóyòng" [Official audit in Guangdong Province reveals that more than 200 million RMB of ear-marked funds for water conservancy had been misappropriated] (27 July 2004) (last visited 10 November 2020), online: *Sina* < finance.sina.com.cn/g/20040727/2142905332.shtml > .

[26] Qian Systematic Framework, *supra* note 5.

C. Solution to the Zero Lower Bound Problem

The "zero lower bound" problem occurs when Central Banks attempt to set a negative interest rate to encourage spending and investment but fail to do so because citizens would simply stop depositing money into banks and choose to hoard hard cash instead.[27] Macroeconomists, such as the Bank of England's Chief Economist, Andrew Haldane, believe that the CBDC is the solution to the "zero lower bound problem" as the Central Bank would retain the power to set a negative interest rate.[28] Max Raskin and David Yermack from the US National Bureau of Economic Research have made similar suggestions of allowing the Central Bank to simply adjust interests on the consumer's accounts.[29] "Economic state contingent," as a subset of the "forward contingents" above-mentioned, has also been proposed to introduce counter-cyclical adjustment to interest rates based on macroeconomic conditions, thereby achieving counter-cyclical control of the economy.[30]

Nevertheless, it should be cautioned that even though this is a theoretically feasible benefit, Central Banks should be cautious in applying a negative interest rate or adjusting interest rates on the CBDC in general, as it would send a signal of excessive control and insecurity among consumers. Setting a negative interest rate should therefore be used sparingly with sufficient forward guidance to the market in order not to generate public resentment against the CBDC. In the case of the DCEP, public support is particularly crucial given it is still a novel concept.

(ii) Lowered Transaction Cost

Secondly, the DCEP lowers transaction costs and greatly speeds up the entire transaction. There would no longer be "shoe leather cost" in terms of making trips to the bank, ATM or physical meet-up. The transaction would be almost instantaneous with a touch of one's finger in his digital wallet. In the context of China, such benefits have already been enjoyed by the public with regard to WeChat Pay and AliPay, and therefore, the public can easily appreciate the convenience brought about by the DCEP.

(iii) Recognition as Legal Tender

Lastly, the DCEP possesses a unique advantage over privately issued cryptocurrencies through its recognition as a legal tender. Legal tender is the

---

[27] Max Raskin & David Yermack, "Digital Currencies, Decentralized Ledgers, and The Future of Central Banking" (2016) National Bureau of Economic Research Working Paper No. 22238 [NBER Digital Currencies], online (pdf): *National Bureau of Economic Research* < www.nber.org/papers/w22238 > .

[28] Andrew Haldane, "How low can you go? — speech by Andrew Haldane" (18 September 2015) (last visited 13 July 2020), online: *Bank of England* < www.bankofengland.co.uk/speech/2015/how-low-can-you-can-go > .

[29] NBER Digital Currencies, *supra* note 27.

[30] Qian Systematic Framework, *supra* note 5.

money that a debtor offers to his creditor in an attempt to discharge his liability, which the creditor is required by law to accept.[31] Like many other jurisdictions,[32] § 16 of the *PBOC Law* and § 3 of the *Renminbi Regulation Rules*[33] prohibit the refusal of legal tender in payment of a debt. Associated with the idea of legal tender is a country's currency right, which refers to the right of the sovereign government to determine the value, types, amount and process of issuing currency based on specific needs and conditions of the country.[34] For instance, § 4.1.3 of the *PRC People's Bank of China Law* specifically authorizes the PBOC to exclusively exercise currency rights to issue and regulate RMB on behalf of the government.[35] Accordingly, the advantage of being recognized as a legal tender also means that a currency's value is supported by and anchored in sovereign credit, with the people's trust in the government helping to stabilize its value and guard against rampant fluctuations as observed in Bitcoin.[36] Therefore, whether a cryptocurrency gains recognition as a legal tender would significantly impact its functionality as a real currency. Suffice it to say that while government-issued CBDC such as the DCEP would certainly be recognized as legal tender, private cryptocurrencies such as Bitcoin and Libra would almost never gain this status.

(c) Legal Issues & Risks of the DCEP

Scholars have identified several potential legal issues that are generally applicable to privately issued cryptocurrencies as well as the DCEP. These issues include 1) counterfeit and cyber attack, and the dilemma between 2) privacy and data protection on one end and 3) combating illegal activities including money laundering, tax evasion and terrorist financing on the other. As will be explained in Section 3, many of these concerns dictate governments', including the Chinese government's reluctance or even aversion towards privately issued cryptocurrencies. As a result, it is crucial for the structural design of the DCEP to be able to resolve these issues.

---

[31] Arthur Nussbaum, *Money in the Law*, revised ed. (Brooklyn, NY: Foundation Press, 1950) at 45. See also the US Legal Tender Cases, *Knox v. Lee; Parker v. Davis*, 79 U.S. 457, 20 L.Ed. 287 (1870).

[32] Antonio Sáinz de Vicuna, "An Institutional Theory of Money" in Mario Giovanoli & Diego Devos, eds., *International Monetary and Financial Law: The Global Crisis* (Oxford: Oxford University Press, 2010) at 517-532.

[33] *Regulations of the People's Republic of China on the Administration of Renminbi*, State Council, R., 2018, § 3 [*RMB Rules*].

[34] Xiangmin Liu, "Yãngháng fãxíng shŭ zì huòbì de fãlü wèntí" [Legal Issues on the Issuance of Digital Currency by People's Bank of China] (2016) 17 China Finance at 17-19 [Liu Legal Issues].

[35] *PRC People's Bank of China Law*, National People's Congress, 1995, § 4.1.3 [*PBOC Law*].

[36] Qian Systematic Framework, *supra* note 5.

(i) Counterfeit & Cyber Attack

Section 19 of the *PBOC Law* and section 31 of the *RMB Rules* defined counterfeit money as forged counterfeit or altered RMB.[37] With the introduction of the DCEP, the methods of counterfeiting are expected to be drastically different from those of hard currency. These methods would be technical and arise via cyber attacking the verification and registration system run by the PBOC, or cracking the DCEP algorithm.[38] In fact, even before the DCEP officially launched, there had already been reported cases of counterfeit DCEP digital wallets.[39] Such fraudulent attempts lure the non-tech-savvy folks who may have heard of the DCEP but are incognizant of any details to make deposits with them. Further, it is argued that given the Central Bank's exclusive control and access over the DCEP algorithm, they may employ a hidden, rather than a conventionally open, blockchain technology. Lack of third-party verification would mean a successful cyber attack on the PBOC would be far more detrimental to the DCEP system than the traditional counterfeit of hard currency, which incurs a relatively limited impact.

In recent history, there have been numerous recorded instances of large-scale cyber attacks on cryptocurrencies. The New York Times and Wall Street Journal reported that Mt. Gox, which was once the world-dominating Bitcoin exchange platform based in Japan that collapsed in February of 2014, had "as much as six percent of the Bitcoins in circulation missing - worth more than $300 million,"[40] and "Mt. Gox lost almost 750,000 Bitcoins in a long-running theft."[41] Similarly, Upbit, a popular South Korean cryptocurrency exchange platform, was attacked by unknown hackers in 2019 with a loss of 342,000 Ethereum worth »37.6 million.[42] Such attacks are often accompanied by loss of user information, suspension of transactions or bankruptcy of the exchange, leaving the users with no recourse to reclaim their funds.[43] According to Group-IB, an international

---

37 *PBOC Law*, *supra* note 35, § 19; *RMB Rules*, *supra* note 33, § 31.

38 *Ibid.*

39 China Securities Journal, "Yãngháng mù chángchūn: Shìchăng shàng yĭ chūxiàn jiămào de shùzì rénmínbì qiánbão" [PBOC Mu Changchun: Counterfeit DCEP Digital Wallets Have Appeared on the Market] (26 October 2020) (last visited 5 November 2020), online: *China Securities Journal* <news.dayoo.com/finance/202010/26/139999_53621496.htm>.

40 Rachel Abrams & Nathaniel Popper, "Trading Site Failure Stirs Ire and Hope for Bitcoin" (25 February 2014) (last visited 13 July 2020), online: *NYTimes* <dealbook.nytimes.com/2014/02/25/trading-site-failure-stirs-ire-and-hope-for-bitcoin>.

41 Robin Sidel, Michael J. Casey & Eleanor Warnock, "Shutdown of Mt. Gox Rattles Bitcoin Market" (26 February 2014) (last visited 13 July 2020), online: *WSJ* <www.wsj.com/articles/bitcoin-website-mt-gox-unavailable-1393305257>.

42 Jay Jay, "Hackers Cart Away »37.6m in Ethereum from South Korean Cryptocurrency Exchange" (28 November 2019) (last visited 13 July 2020), online: *Teiss* <www.teiss.co.uk/ethereum-theft-upbit/>.

43 *Ibid.*

company specializing in preventing cyber attacks, at least 14 cyber attacks on crypto exchanges happened in 2017, resulting in a loss of $882 million, with five of these attacks linked to the notorious Lazarus gang and allegedly sponsored by the North Korea government.[44]

Even conventional electronic transfer service providers like Visa and MasterCard have not been able to completely rid themselves of malicious cyber attacks. From time to time, the Payment Fraud Disruption Department at Visa would warn users of attacks targeted at their Points-of-Sale (POS) machines, with malware implanted by hackers stealing customers' payment card data.[45] In China, the theft and duplication of bank card information has also been a long-standing concern.[46] Even the most recent contactless payment methods like PayWave raise concerns about electronic pickpocketing using POS machines or simply handphones with malware.[47]

If a major attack on the DCEP system was successful, apart from monetary loss and potential loss of transactional and personal information of the users, the Chinese government and its Central Bank would also stand to lose public confidence. Furthermore, unlike cryptocurrency exchanges, with the option of suspension of transactions or even bankruptcy, once the DCEP is up and running, it is almost inconceivable for PBOC to temporarily halt its usage even when its database is under attack. Any suspension of a considerable length of time would disrupt millions of transactions, create fear among the public that their digital currency may lose its value and possibly lead to a bank run to convert their DCEP back to conventional fiat currency, adding even more workload to the overwhelmed system. This means that the design of the DCEP has to be even more secure and robust than privately issued cryptocurrencies.

(ii) The Dilemma Between Anonymity and the Real Name System

The twin problem of personal data protection and fulfilment of its anti-money-laundering (AML) and counter-terrorist-finance (CTF) obligations means that the design of the DCEP needs to strike a balance between anonymity and registration of users on a real-name basis. Blanket anonymity would render the DCEP a digital haven for money-laundering and other illegal

---

[44] Group-IB, "14 cyber attacks on crypto exchanges resulted in a loss of $882 million" (17 October 2018) (last visited 13 July 2020), online: *GroupIB* < www.group-ib.com/media/gib-crypto-summary/ > .

[45] Lifars, "Beware of New POS Attack, Warned Visa" (1 December 2020) (last visited 13 July 2020), online: *Lifars* < lifars.com/2020/01/beware-of-new-pos-attack-warned-visa/ > .

[46] Xinhua News, "Yínháng kǎ bèi dào shuā zěnme bàn? Zhèyàng zuò kě bìmiǎn sǔnshī jìnyībù kuòdà" [What To Do With Unauthorized Use of Your Bank Card? Steps To Avoid Further Losses] (11 June 2018) (last visited 13 July 2020), online: *Xinhua News* < www.xinhuanet.com/2018-06/11/c_1122968147.htm > .

[47] Thomas Bocek et al., "An NFC Relay Attack with Off-the-shelf Hardware and Software" in Rémi Badonnel et al., eds., *Management and Security in the Age of Hyperconnectivity* (Springer, 2016).

acts, whereas a wholesale real-name system exacerbates the risks of data leakage by intermediaries to ill-minded parties.

A. Privacy and Data Protection

The fact that the DCEP is stored in purely digital form, with its ownership primarily determined by identification codes and private keys of the owner, and its transfer effected by information transmission, means the DCEP, compared to hard currency, faces even greater challenges when it comes to personal information protection.[48] In this regard, hard currency carries a greater level of anonymity, as the money itself does not carry information of its previous holder.[49] Once the personal identification codes and private keys are lost, the damage to the target is two-fold. Firstly, in terms of the exposure of his privacy, and secondly, in the loss of his property rights, as the hacker could easily gain ownership of the target's digital money.[50]

Take the European *General Data Protection Regulation*[51] as reference (since the *PRC Personal Date Protection Law* is still being drafted), a few important aspects of personal data protection would include 1) the identification and obligations of the data controllers and processors.[52] In the case of the DCEP, this would include the PBOC, commercial banks and merchants, app developers and third-party contractors. 2) the identification of the processing and usage of the data necessary for the provision of services,[53] and 3) the rights of data subjects, in particular, the right to erasure data after a certain period to prevent misuse.[54]

Furthermore, a potential attack could theoretically happen at multiple levels; on the PBOC digital verification services centre, on the customer's digital wallet or on the terminal maintained by merchants and commercial banks, aggravating the possibility of an attack. In this regard, it is recommended that legislation should quickly catch up by criminalizing and prohibiting any form of unauthorized solicitation or collection of personal identification information of DCEP account owners, including the amount of DCEP held, private keys and transaction history, making such information strictly confidential.[55] However, just like the existing cases of massive leakage of personal data from mega corporations and government bodies, the fear is that legislation *per se* is not

---

48 Liu Legal Issues, *supra* note 34.

49 Qian Systematic Framework, *supra* note 5.

50 Liu Legal Issues, *supra* note 34.

51 *Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, EU Reg. 679/2016 [*General Data Protection Regulation*].

52 *Ibid*., Chapter 2.

53 *Ibid*., § 6.

54 *Ibid*., Chapter 3, § 17.

55 Liu Legal Issues, *supra* note 34.

sufficient to deter criminal-minded hackers who are skillful enough to hide their traces.

Loss of personal information through cyber attacks has been a real concern in China.[56] It is more worrying given that the relevant regulations are sparse,[57] and the *PRC Personal Information Protection Law* is still being drafted.[58] Despite the State Council's *Notification on Major Points of Administrative Matters in 2018* making explicit instruction for government agencies at all levels to make their best effort in personal data protection,[59] Xinhua News reported that:

> [P]ersonal information is still leaked from local governments and departments. Such leakage is particularly prevalent through the public disclosure of information concerning poor households, poverty alleviation lists, households receiving government subsidies, reconstruction of dilapidated houses and resettlement. Some administrative websites not only disclose personal information, but allow open download of essential personal information.[60]

In the shocking case, informally known as *Death of Xu Yuyu Caused by Telecom Fraud*,[61] the accused persons illegally purchased from hackers more than 100,000 pieces of information concerning the students attending that year's University Entrance Examination in Shandong province. They then picked low-income students like Xu Yuyu, called her up and pretended to be the Ministry of Education, offering her a bursary and requiring her to transfer 10,000 RMB in advance to activate her account. She transferred the money intended to cover her school fees, only to realize it was a fraud much later. On her way back from the police station, she collapsed and died out of despair and exhaustion.[62] In total,

---

[56] Zhang Huaiyin, "Dà shùjù shídài de gèrén xìnxī bǎohù tànxī" [A Probe into Personal Information Protection in the Era of Big Data] (19 September 2019) (last visited 13 July 2020), online: *Xinhua* < www.xinhuanet.com/info/2019-09/19/c_138403840.htm > .

[57] See discussion in Section V.C. below.

[58] Xinhua, "Quánguó réndà chángwěi huì fǎ gōng wěi: Gèrén xìnxī bǎohù fǎ zhèngzài yánjiū qǐcǎo zhōng" [National People's Congress Legal Work Committee: In the Process of Drafting Personal Information Protection Law] (14 May 2020) (last visited 13 July 2020), online: *Xinhua* < www.xinhuanet.com/legal/2020-05/14/c_1125986394.htm > .

[59] China, State Council, *Notification on Printing and Issuing Major Points of Administrative Matters in 2018 by State Council*, No. 23 (State Council, 2018), § 14.

[60] Xinhua, "Zhèngfǔ bùmén yǐng chéngwéi gèrén xìnxī bǎohù diǎnfàn" [Government Department Should be Role Models for Personal Information Protection] (7 May 2018) (last visited 13 July 2020), online: *Xinhua* < www.xinhuanet.com/comments/2018-05/07/c_1122791736.htm > .

[61] *Fraud & Intrusion of Citizen's Personal Information by Chen Wenhui, Zhen Jinfeng and Others*, 2017 Shandong People's High Court No. 281 (281).

[62] China, Supreme People's Procuratorate, "Gōngsùrén xiángjiě xúyùyù bèi diànxìn zhàpiàn zhìsǐ àn bàn'àn lìchéng" [Prosecutor Reveals Details on the Death of Xu Yuyu Caused by Telecom Fraud] (27 June 2017) (last visited 13 July 2020), online: *Supreme People's Procuratorate* < www.spp.gov.cn/zdgz/201706/t20170627_194085.shtml > .

the accused persons called up 23,000 students and obtained 560,000 RMB through fraud and were eventually sentenced to life imprisonment.[63]

Prominent examples of leakage of personal information from huge corporations include the theft of more than one billion pieces of personal data from internet giants such as Tencent and Sina by the dark web supplier DoubleFlag,[64] loss of one billion pieces of data by parcel delivery giant YTO Express[65] and half a billion pieces of data by hospitality company Marriott International.[66] The strong linkage between fraud cases and leaked personal information in China, together with the varied educational level of DCEP users, highlights the seriousness of personal data protection in designing the DCEP.

B. AML, CTF and Other Illegal Activities

The anonymity and cross-boundary features of the existing privately issued cryptocurrencies have made them attractive to the criminal underworld in facilitating their transactions and laundering criminal proceeds.[67] While more empirical examples of the illegal activities spurred by cryptocurrencies will be explained in the next section on Bitcoin, the greatest concern is still with money-laundering. In China, the AML legal framework is governed by the *PRC Anti-Money-Laundering Law*[68] and a series of regulations such as the *Anti-Money-Laundering Regulations on Financial Institutions*.[69] Under this legal framework, PBOC is the primary regulatory and executive body overseeing AML activities in China. Financial and other specified institutions are responsible for conducting identity checks on their clients and reporting large-sum or suspicious transactions. The China Anti-Money-Laundering Inspection and Analysis Centre is responsible for analyzing transaction data.[70]

The issuance of DCEP poses multiple challenges to this framework. Firstly, compared to hard currency, DCEP is easier to transfer large amounts. The transaction is harder to detect because even though there is a digital record, it may not ring an alarm bell if the transacting parties were not already being watched. Secondly, the DCEP reduces transacting parties' reliance on financial

---

63 *Fraud & Intrusion of Citizen's Personal Information by Chen Wenhui, Zhen Jinfeng and Others*, *supra* note 61.

64 Sina, "Duō jiā zhōngguó hùliánwǎng gōngsī dàliàng bèi dào zhànghù zài àn wǎng xiāoshòu" [A Large Number of Stolen Accounts of Many Chinese Internet Companies are Sold on the Dark Web] (4 February 2017) (last visited 13 July 2020), online: *Sina* <t.cj.sina.com.cn/articles/view/5616949402/14ecbd89a019001d87>.

65 Huaiyin, *supra* note 56.

66 *Ibid.*

67 Lawrence Trautman, "Virtual Currencies: Bitcoin & What Now after Liberty Reserve, Silk Road and Mt. Gox?" (2014) 20 Richmond Journal of Law & Technology 13.

68 *PRC Anti-Money-Laundering Law*, National People's Congress, 2006.

69 *Anti-Money-Laundering Regulations on Financial Institutions*, People's Bank of China, 2006.

70 Liu Legal Issues, *supra* note 34.

and other institutions. More transactions will be carried out on a peer-to-peer (P2P) level outside of the financial system, weakening institutions' abilities to perform their existing monitoring and reporting of suspicious activities.[71] A similar analysis applies to other illegal activities conducted via cryptocurrency transaction platforms, such as terrorist financing and payment for illegal transactions such as assassins-for-hire or corporate espionage.

3. CHINA'S APPROACH TO BITCOIN AND FACEBOOK'S LIBRA

(a) Basic Information on Bitcoin

Since its inception in the renowned 2008 paper by Nakamoto, Bitcoin was designed to be a "Peer to Peer Electronic Cash System," which allows network members to transfer value directly between each other without the need of a trusted third-party such as the Central Bank, making Bitcoin a direct competitor of fiat currency.[72] Bitcoin was able to achieve such decentralized governance, record keeping and verification because of the underlying blockchain and DLT.

In essence, Bitcoin uses the P2P network to group the transaction information within a certain time period together with their time stamps to form an information "block," and then links the "blocks" together chronologically to form a "blockchain," with each "block" carrying a summary of the key information contained in the previous "block." As such, the sequence of the blockchain is unalterable once it is formed.[73] This blockchain is then known as a "distributed ledger" once it is made available to all members of the network, with each one of them playing an important function of validating and verifying its authenticity. This system prevents a single rouge user from maliciously manipulating the data since their record would be different from the rest.[74]

In terms of issuance, Bitcoin can either be acquired in a transaction by exchanging goods and services for Bitcoins or as a reward for "mining," in which the users update the network's blockchain. Notably, unlike fiat currency, there is a cap on money creation of 21 million Bitcoins, and no new Bitcoin will be introduced after 2140.[75]

(b) Bitcoin and Illegal Activities

Bitcoin and similar cryptocurrencies possess a few characteristics that make them preferable to criminals, including 1) a high level of anonymity, 2) ability to move funds quickly and stealthily across jurisdictions to evade tracking by law

---

[71] *Ibid.*

[72] Nakamoto, *supra* note 1.

[73] Qian Conceptual Prototype, *supra* note 14.

[74] NBER Digital Currencies, *supra* note 27.

[75] *Ibid.*

enforcement, 3) widespread adoption in the criminal underground and 4) high trustworthiness by criminals.[76] Given these characteristics, scholars observed that "Bitcoin is a disruptive technology that undermines the regulatory capacity of the state."[77]

Bitcoin has been extensively criticized for its facilitation of money laundering,[78] which has been aggravated by the introduction of Bitcoin ATM,[79] and difficulties experienced trying to regulate Bitcoin senders, launderers and processors.[80] Those who launder money using Bitcoin are often criminals engaging in numerous types of criminal activities such as facilitating marketplaces for assassins, corporate espionage and hostile attacks, child pornography, drugs, fake personal identification documents, Ponzi schemes and other financial frauds, credit card frauds and the illegal sale of weapons.[81] The remarkable instances of large-scale crackdowns by the FBI and US Department of Justice included the shut-down and seizure of Liberty Reserve, Silk Road and Freedom Hosting in 2013 and 2014.

Liberty Reserve was a major digital currency service provider using its own cryptocurrency called the Liberty Reserve. Specifically designed with multiple layers of anonymity, such as acceptance of the registration by fictitious names and use of third-party exchanges to avoid collecting any meaningful information about its users, Liberty Reserve was intentionally designed to evade law enforcement and marketed itself as "the bank of choice for the criminal underworld."[82] A press release by the US Department of Justice showed that "before being shut down by the US government in May 2013, Liberty Reserve had more than *five million users* worldwide"[83] and "allegedly *laundered more than*

---

[76] US Senate Committee on Homeland Security and Governmental Affaris, *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies*, S.Hrg. 113-516 (Washington: US Government Printing Office, 2013), Testimony of Edward W. Lowery III, Special Agent in Charge, Criminal Investigative Division, US Secret Service, US Department of Homeland Security [*Beyond Silk Road*].

[77] Gabriel J. Michael, "Anarchy and Property Rights in the Virtual World: How Disruptive Technologies Undermine the State and Ensure that the Virtual World Remains a 'Wild West'" (1 March 2013), online (pdf): *SSRN* < papers.ssrn.com/sol3/papers.cfm?abstract_id = 2233374 > .

[78] Sheng Zhou, "Bitcoin Laundromats for Dirty Money: The Bank Secrecy Act's Inadequacies in Regulating and Enforcing Money Laundering Laws over Virtual Currencies and the Internet" (2014) 3:1 J.L. & Cyber Warfare at 103-142.

[79] Mitchell Hyman, "Bitcoin ATM: A Criminal's Laundromat for Cleaning Money" (2015) 27:2 St.Thomas Law Review at 296-317.

[80] Danton Bryans, "Bitcoin and Money Laundering: Mining for an Effective Solution" (2014) 89:1 Ind. L.J. at 441-472.

[81] Trautman, *supra* note 67 at 8; Fernando M. Pinguelo & Bradford W. Muller, "Virtual Crimes, Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals" (2011) 16:1 Va. J.L.& Tech. 116 at 119.

[82] *United States v. Liberty Reserve*, 13 C.R. 368 (S.D. N.Y., 2015) [*United States v. Liberty Reserve*].

$6 billion in suspected proceeds of crimes, including credit card fraud, identity theft, investment fraud, computer hacking, child pornography and narcotics trafficking."[84] Its founders eventually pled guilty to these charges.[85] The criminal operations supported by Liberty Reserve were present in jurisdictions including the US, China, Hong Kong, Vietnam and Nigeria, while Liberty Reserve stored their funds in many more countries.[86]

Similarly, Silk Road, a transaction infrastructure platform using Bitcoin as its currency, was nicknamed "the Amazon for Drugs"[87] and described as "the most sophisticated and extensive criminal marketplace on the Internet."[88] In particular, users of Silk Road were able to purchase illegal drugs of every kind under the disguise of anonymity using untraceable currency like Bitcoin and shipping through a sprawling network of illicit suppliers around the world to their doorsteps. In its short lifespan of two and a half years, hundreds of kilograms of drugs were distributed via Silk Road,[89] and over 173,991 Bitcoins worth over $33.6 million were seized by law enforcement from the website.[90] Around the same period, the web hosting service Freedom Hosting maintained several child pornography sites, with an estimated 15,000 members and 1.5 million child pornography images. All of these sites accepted Bitcoins for

---

83 US Department of Justice, "Founder of Liberty Reserve Arthur Budovsky Pleads Guilty in Manhattan Federal Court to Laundering Hundreds of Millions of Dollars Through his Global Digital Currency Business" (29 January 2016) (last visited 13 July 2020), online: *DOJ* < www.justice.gov/usao-sdny/pr/founder-liberty-reserve-arthur-budovsky-pleads-guilty-manhattan-federal-court > .

84 US Department of Justice, "Co-Founder of Liberty Reserve Pleads Guilty to Money Laundering in Manhattan Federal Court" (1 November 2013) (last visited 13 July 2020), online: *DOJ* < www.justice.gov/usao-sdny/pr/co-founder-liberty-reserve-pleads-guilty-money-laundering-manhattan-federal-court > .

85 *Ibid.*

86 *United States v. Liberty Reserve*, *supra* note 82.

87 *Beyond Silk Road*, *supra* note 76, Testimony of Ernie Allen, President & Chief Executive Officer, The International Centre for Missing & Exploited Children.

88 US Attorney's Office for the Southern District of New York, "Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of 'Silk Road' Website" (25 October 2013) (last visited 13 July 2020), online: *FBI* < archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website#:~:text = Share-,Manhattan%20U.S.%20Attorney%20Announces%20Seizure%20of%20Additional%20%2428%20Million%20Worth,Bitcoins%20Worth%20Over%20%2433.6%20Million > .

89 *Ibid.*

90 Charles E. Schumer & Joe Manchin, "Manchin Urges Federal Law Enforcement to Shut Down Online Black Market for Illegal Drugs" (6 June 2011), online: *Joe Manchin United States Senator* < www.manchin.senate.gov/newsroom/press-releases/manchin-urges-federal-law-enforcement-to-shut-down-online-black-market-for-illegal-drugs > .

payment and, therefore, shifted criminal activities to an unregulated economy backed by cryptocurrencies.[91]

Many of the above-mentioned digital platforms were able to achieve a level of almost absolute anonymity with a number of cryptographic tools such as the anonymous proxy network Tor, short for "The Onion Routing" project, and initially developed by the US Naval Research Laboratory.[92] In essence, the Tor mechanism sends information about a transaction over a series of nodes on the internet, with the effect that each node only knows the identity of the one node before and after itself in the chain and could never link the actual sender of the information to its final receiver.[93] These instances demonstrated that the key features of Bitcoin and associated cryptographic tools, such as anonymity, cross-border transactions, lack of third-party supervision and easiness to transmit and conceal criminal proceeds, have rendered them fertile grounds for criminal activities of all kinds. Those activities are more hidden, more cross-border in nature and require greater collaboration between law enforcement agents in different countries to bring them to justice.

(c) Ban of Bitcoin in China

Surprisingly, before the Chinese government's subsequent crackdown, there was a brief period of rampant Bitcoin activities in China. It was reported by China Daily that in November 2013, "China transacts *half of the global Bitcoin volume*"[94] and "an estimated 1.8 million Bitcoins were traded on BTC China in November, the platform with the highest trading volume in the world."[95] This exceedingly high volume of usage in light of the emergence of the extensive criminal networks naturally worried the Chinese government. Furthermore, while Bitcoin is certainly not a legal tender, it nevertheless poses a great threat to a Central Bank's ability to conduct monetary policy as a monopolist. This is particularly worrying for the PBOC, given that the Chinese government imposes capital control policies, and the PBOC actively engages in market intervention to affect the value of the RMB.

---

91 *Beyond Silk Road*, *supra* note 76, Testimony of Ernie Allen, President & Chief Executive Officer, The International Centre for Missing & Exploited Children.

92 Todd G. Shipley & Art Bowker, "Chapter 9 - Working Unseen on the Internet" in Todd G. Shipley & Art Bowker, eds., *Investigating Internet Crimes* (Amsterdam: Elsevier, 2014) at 219-225.

93 Roger Dingledine, Nick Mathewson & Paul Syverson, "Tor: The Second-Generation Onion Router" (last visited 13 July 2020), online (pdf): *Naval Research Lab* <www.onion-router.net/Publications/tor-design.pdf>.

94 John Coulter, "Beware of the Baneful Bitcoin Bug" (29 November 2013) (last visited 13 July 2020), online: *China Daily* <www.chinadaily.com.cn/opinion/2013-11/29/content_17139203.html>.

95 Xinhua, "China Becomes Largest Bitcoin Market" (5 December 2013), online: *China Daily* <www.chinadaily.com.cn/business/2013-12/05/content_17153347.htm>.

Due to these above-mentioned concerns, transactions using Bitcoin are banned in China. In December 2013, the PBOC, together with China Securities Regulation Commission, China Banking Regulatory Commission, China Insurance Regulatory Commission and the Ministry of Industry and Information Technology, jointly issued the *Notice on Precautions Against the Risks of Bitcoins*.[96]

In this *Bitcoin Notice*, Bitcoin is defined as "a virtual commodity and not a real currency" due to its lack of status as a legal tender. Accordingly, *it is prohibited from being circulated and used as a currency in the market*.[97] Banks and other financial and payment institutions are prohibited from dealing in Bitcoins, and:

> [F]inancial and payment institutions should not use Bitcoin pricing for products and services, buy or sell Bitcoins, or provide direct or indirect Bitcoin-related services to customers, including registering, trading, settling, clearing, or other services; accepting Bitcoins or using Bitcoins as a clearing tool; and trading Bitcoins with RMB or foreign currencies.[98]

Subsequently, in April 2014, the PBOC ordered commercial banks and trading companies to shut down accounts that dealt in Bitcoin, and in 2017, Bitcoin exchanges were also shut down.[99] The *Bitcoin Notice* also specifically warned against the risks of the Bitcoin system being used for money laundering due to its anonymous and transboundary characteristics.[100]

This can be contrasted with the more liberal approach in other jurisdictions.[101] For example, the United Kingdom (UK) allows the private use of Bitcoin as well as the opening of businesses that transact in Bitcoins. A number of officials in the US government have similarly leaned towards an attitude of "benign neglect" towards Bitcoin and other digital currencies.[102] Even

---

[96] China, PBOC, CSRC, CBRC & CIRC, *Notice on Precautions Against the Risks of Bitcoins*, No. 289 (PBOC, CSRC, CBRC & CIRC, 3 December 2013) [*Bitcoin Notice*].

[97] *Ibid*., § 1.

[98] *Ibid*., § 2.

[99] Chao Deng & Lingling Wei, "China Cracks Down on Bitcoin" (1 April 2014) (last visited 13 July 2020), online: *WSJ* < www.wsj.com/articles/china-cracks-down-on-bitcoin-1396361492?tesla = y > ; Chao Deng & Paul Vigna, "China to Shut Bitcoin Exchanges" (11 September 2011) (last visited 13 July 2020), online: *WSJ* < www.wsj.com/articles/china-to-shut-bitcoin-exchanges-sources-1505100862 > .

[100] *Bitcoin Notice*, *supra* note 96, § 4.

[101] See an excellent summary of Bitcoin's treatment in various jurisdictions at US Library of Congress, "Regulation of Bitcoin in Selected Jurisdictions" (last visited 13 July 2020), online: *Library of Congress* < www.loc.gov/law/help/bitcoin-survey/ > .

[102] NBER Digital Currencies, *supra* note 27; see also Max Raskin, "U.S. Agencies to Say Bitcoins Offer Legitimate Benefits" (19 November 2013) (last visited 13 July 2020), online: *Bloomberg* < www.bloomberg.com/news/articles/2013-11-18/u-s-agencies-to-say-bitcoins-offer-legitimate-benefits > .

though both countries have AML laws, neither deem it necessary to ban Bitcoin or prevent its proliferation for that purpose.

(d) Basic Information on Libra

When Facebook announced its Libra project on 18 June 2019, it was envisioned as "a simple global currency and financial infrastructure that empowers billions of people."[103] There are three essential features of Libra that account for most of its unique characteristics, "1) It is built on a secure, scalable and reliable *blockchain*; 2) it is *backed by a reserve of assets* designed to give it *intrinsic value*; 3) it is *governed by the independent Libra Association* tasked with evolving the ecosystem."[104] The Libra Blockchain is able to support a much higher transaction volume (1000 transactions per second) compared to other cryptocurrencies such as Bitcoin (only seven transactions per second), allowing its use to scale to billions of accounts.[105] At the same time, "Libra Blockchain is pseudonymous and allows users to hold one or more addresses that are not linked to their real-world identity,"[106] opening up concerns with encouraging illegal activities including tax evasion, money laundering and terrorist financing.

A major difference between Libra and other cryptocurrencies that lack intrinsic value is the fact that Libra is designed to guard against extreme value fluctuation as exhibited in Bitcoin by being backed by a reserve of real low-volatility assets, such as bank deposits and short-term government securities in currencies issued by reputable Central Banks.[107] A further announcement by Facebook confirmed that the Libra currency basket will include 50% USD, 18% EUR, 14% JPY, 11% GBP and 7% SGD,[108] with no Chinese RMB at the particular request of Senator Mark Warner out of concerns with potential currency manipulation.[109]

New Libra coins are only created when buyers purchase those coins from the Libra Association with real assets to back the intrinsic value of the new coins. Libra coins are only destroyed when the buyers sell their Libra coins to the

---

[103] Libra White Paper, *supra* note 5.

[104] *Ibid.*

[105] Bernard Marr, "Facebook's Blockchain-Based Cryptocurrency Libra: Everything You Need to Know" (7 October 2019) (last visited 13 July 2020), online: *Forbes* < www.forbes.com/sites/bernardmarr/2019/10/07/facebooks-blockchain-based-cryptocurrency-libra-everything-you-need-to-know/#661d95744d7a > .

[106] Libra White Paper, *supra* note 5.

[107] *Ibid.*

[108] Steven Zheng, "Facebook Libra will be made up of U.S. dollar, euro, yen, pound, and Singapore dollar" (21 September 2019) (last visited 13 July 2020), online: *Yahoo* < finance.yahoo.com/news/facebook-libra-made-u-dollar-205718144.html > .

[109] Joe Light, "Facebook Sees Libra Tied to Dollar Euro, Yen But Maybe Not Yuan" (10 September 2019) (last visited 13 July 2020), online: *Bloomberg* < www.bloomberg.com/news/articles/2019-09-09/facebook-sees-libra-tied-to-dollar-euro-yen-but-maybe-not-yuan > .

reserve at a price equal to the basket of real assets. However, granted that Libra has committed to holding the most secure and reliable assets, the value of the assets is still prone to variation following recession and expansion in the real economy and therefore, the exchange rate between Libra and other fiat currencies can still vary to some extent.[110]

The Libra Association is the governing body of Libra and the only party with the power to create and destroy Libra.[111] In its initial June 2019 announcement, members of the Libra Association included major players in the FinTech, e-commerce and payment space such as PayPal, Visa, MasterCard, eBay, Spotify and Uber. However, in October 2019, after PayPal being the first to back out, a few other companies joined the exit list, including Visa, MasterCard and Stripe.[112] Notably, not a single bank has shown support for the Libra project as they felt their own multi-billion-dollar payment businesses were threatened by Libra. Large brick-and-mortar retailers such as Walmart did not join as well for concern over consumer adoption of Libra.[113]

(e) Potential Disruption and Challenges Posed by Libra

Facebook alone has 2.4 billion users worldwide, eight times that of the US population, not to mention the users of Instagram, WhatsApp and other platforms belonging to Facebook.[114] With its ambition of becoming a global leader in digital coin payments and rivalling Central Bank fiat currencies, even if a portion of its users switch from using fiat currency to Libra, the disruption to the established global monetary system would be unprecedented.[115] This is because the wide userbase of Facebook provides a strong potential global acceptance of Libra as a currency given its promised efficiency, low transaction cost and most importantly, transboundary features. At a certain point, when millions of users get used to passing on Libra coins unlimitedly in transactions, Libra becomes much similar to the conventional fiat currency in its own regard, and the underlying redemption option against the reserve of assets becomes

---

[110] *Ibid.*

[111] *Ibid.*

[112] Lauren Feiner, "Facebook's Libra Cryptocurrency Coalition is Falling Apart as eBay, Visa, Mastercard and Stripe jump ship" (11 October 2019) (last visited 13 July 2020), online: *CNBC* < www.cnbc.com/2019/10/11/ebay-drops-out-of-facebook-libra-crypto-currency-one-week-after-paypal.html > .

[113] Jennifer Surane, Julie Verhage & Kurt Wagner, "Facebook's Cryptocurrency Project: Who's In and Who's Out" (18 June 2019) (last visited 13 July 2020), online: *Bloomberg* < www.bloomberg.com/news/articles/2019-06-18/facebook-s-cryptocurrency-project-who-s-in-and-who-s-out > .

[114] Statista, "Leading Countries Based on Number of Facebook Users as of January 2020" (January 2020) (last visited 13 July 2020), online: *Statista* < www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/ > .

[115] Christian Hofmann, "The Changing Concept of Money: A Threat to the Monetary System or an Opportunity for the Financial Sector?" (2020) 21 Eur. Bus. Org. L. Rev., online: *Springer* < doi.org/10.1007/s40804-020-00182-z > .

obsolete and meaningless, as users would rather make payment directly in Libra coins.[116] When this happens, there could even be a de-link between Libra and the reserve of assets, where Libra coins become only redeemable in Libra coins itself and nothing else, much like when Central Bank fiat currencies de-linked from the gold reserves as the Bretton Woods system fell. At that stage, Libra, as a privately issued cryptocurrency, would directly compete with Central Bank fiat currencies and cause major disturbance to sovereign countries' abilities to conduct effective monetary policies.[117]

Furthermore, despite the promised high liquidity and low volatility of the underlying reserve of assets, the Libra project, largely a novel unregulated concept, still raises concerns with shadow-banking. Professor Christian Hofmann has likened the Libra system with money market funds as both hold high-quality short-term securities. Just like Libra coins, units in the money market funds can also be converted to fiat currencies.[118] Similar to how money market funds raised shadow banking concerns before regulatory reforms after the 2007 global financial crisis, the Libra concept may incur the same liquidity problems if changes in the real economy drastically decreased trust in Libra and triggered a redemption rush similar to a bank run.

Other issues have also been identified. Scholars pointed out that personal data protection concerns are present at multiple levels for Libra, including transaction data stored in the blockchain, users' personal information stored by the Libra Association and information stored by third-party service providers.[119] There is also a conflict of interest where Facebook, on the one hand, monitors transactional data via Libra and, on the other hand, reaps handsome benefits from advertisements on social media, opening up a possibility of anti-competitive behaviours.[120] Overall, the Libra proposal, as it stands, conjures a series of economic, financial and technological risks for regulators.

(f) Cautious Reaction by the US, Chinese and other Authorities

Given the above serious concerns, it was no wonder that the US regulators have shown a more-than-cautious attitude towards the development of Libra. As early as September 2019, US Treasury warned that Libra had to meet tough AML and CTF standards and accordingly required Libra exchanges to register the real identity of people who changed their fiat currencies into Libra.[121] In

---

[116] *Ibid.*

[117] *Ibid.*

[118] *Ibid.*

[119] Abraham & Guegan, *supra* note 19.

[120] *Ibid.*

[121] Brenna Hughes Negahaiwi, "Swiss-based Libra will have to meet tough U.S. standards: US Treasury" (10 September 2019) (last visited 13 July 2020), online: *Reuters* <www.reuters.com/article/us-facebook-cryptocurrency/libra-cryptocurrency-must-meet-tough-regulatory-standards-u-s-treasury-idINKCN1VV1BT?edition-redirect=in>.

October 2019, Lael Brainard, Governor of the US Federal Reserve, laid out "a core set of legal and regulatory challenges" that Facebook must overcome before Libra can be allowed to operate.[122] On top of her priority list were issues concerning money laundering, consumer protection against value fluctuations and unregulated shadow-banking activities.[123]

At the same time, the US House Committee on Financial Services questioned Facebook's ability to safeguard users' personal information after the Cambridge Analytics saga in addition to potential antitrust concerns arising from a scenario where Facebook would reap profits from advertisements on the one hand and monitor transaction data via Libra on the other.[124] Two Senators wrote a letter to Visa, MasterCard and Stripe, expressly warning them of the risk of their involvement in the Libra project, citing competition and challenges to their own payment businesses from Libra, leading to their eventual exit.[125] Under all these regulatory pressures, Facebook CEO Mark Zuckerberg himself conceded during the historic congress hearing that "the Libra system will not launch in the US or anywhere in the world without approval from US regulators."[126] In this regard, Facebook can perhaps take a leaf from how the SEC was able to challenge and suspend the unregistered issuance of Grams by Telegram, with a penalty of $18.5 million.[127]

The cautionary and rejective sentiment of the US government seems to be shared by Central Banks and regulators around the world, including the European Central Bank,[128] Bank of England,[129] Bank of Japan,[130] Monetary

---

[122] Kiran Stacey, Brendan Greeley & Hannah Murphy, "Federal Reserve Sets Out Regulatory Challenges Facing Facebook's Libra", *Financial Times* (17 October 2019) < www.ft.com/content/ef650f9a-f052-11e9-ad1e-4367d8281195 > .

[123] *Ibid.*

[124] Amy Leisinger, "Zuckerberg defends Facebook, Libra before Financial Services Committee" (23 October 2019) (last visited 13 July 2020), online: *Wolters Kluwer* < lrus.wolterskluwer.com/news/banking-finance/zuckerberg-defends-facebook-libra-before-financial-services-committee/97798/ > .

[125] Lydia Beyoud, & Joe Light, "Senators Caution Mastercard, Visa, Stripe on Libra Membership" (9 October 2019) (last visited 13 July 2020), online: *Bloomberg* < www.bloomberg.com/news/articles/2019-10-09/senators-caution-mastercard-visa-stripe-on-libra-membership > .

[126] Jason Abbruzzese & Jo Ling Kent, "Facebook's Zuckerberg says Libra won't launch without U.S. approval" (23 October 2019) (last visited 13 July 2020), online: *NBC News* < www.nbcnews.com/tech/tech-news/facebook-s-zuckerberg-says-libra-won-t-launch-without-u-n1070561 > .

[127] US Securities and Exchange Commission, Press Release, 2020-146, "Telegram to Return $1.2 Billion to Investors and Pay $18.5 Million Penalty to Settle SEC Charges" (26 June 2020) (last visited 13 July 2020), online: *SEC* < www.sec.gov/news/press-release/2020-146 > .

[128] Andrew Munro, "European central banks reject Facebook Libra, accelerate digital currency plans" (16 September 2019) (last visited 13 July 2020), online: *Finder* < www.finder.com.au/european-central-banks-reject-facebook-libra-accelerate-digital-currency-plans > . See also France, Ministry of the Economy and Finance, &

Authority of Singapore,[131] IMF, World Bank and the Bank for International Settlements.[132] The Swiss Financial Market Supervisory Authority, (FINMA), has also expressed the need for Libra to be subject to licensing requirements and AML obligations.[133]

Turning back to the Chinese authorities' response to the Libra development, it appears that Libra was viewed as a significant competitor to the DCEP in terms of developing the first global digital currency, and China sped up its development of the DCEP after Libra was announced.[134] In July 2019, the Director of the PBOC's Research Bureau, Wang Xin, announced concerns about Libra's ramifications on monetary policies, financial stability and the international financial system. Particularly, the Director cautioned against the scenario of a coexistence between the sovereign currency and Libra with 50% of its reserve backed by USD, stating that the DCEP would step up its progress.[135]

Some Chinese observers expressed optimism about DCEP's advantages over Libra. The Deputy Chairman of the China Centre for International Economic Exchanges, Huang Qifan, pronounced in his speech during the 2019 BUND Summit that Libra was unlikely to succeed due to its lack of support by sovereign credit, lack of legal and regulatory basis for its issuance, potential value

---

Germany, Federal Ministry of Finance, "Joint Statement on Libra" (13 September 2019), online (pdf): *Government of France* <www.gouvernement.fr/sites/default/files/locale/piece-jointe/2019/09/1417_-_joint_statement_on_libra_final.pdf>, where it is stated that "the Libra project, as set out in Facebook's blueprint, fails to convince that those risks will be properly addressed."

129 Caroline Binham, "Bank of England warns Facebook that Libra faces tough oversight" (9 October 2019) (last visited 13 July 2020), online: *Financial Times* <www.ft.com/content/7df7fa22-ea6f-11e9-a240-3b065ef5fc55>.

130 Daniel Palmer, "Now Japanese Regulators Are Getting Anxious About Facebook's Cryptocurrency" (3 July 2019) (last visited 13 July 2020), online: *Coindesk* <www.coindesk.com/now-japanese-regulators-are-getting-anxious-about-facebooks-cryptocurrency>.

131 Omar Faridi, "Singapore's Monetary Authority Head Ravi Menon Says Libra Raises Global Financial Risks" (21 September 2019) (last visited 13 July 2020), online: *Crowd Fund Insider* <www.crowdfundinsider.com/2019/09/151845-singapores-monetary-authority-head-ravi-menon-says-libra-raises-global-financial-risks/>.

132 Abraham & Guegan, *supra* note 19.

133 Switzerland, FINMA, "FINMA publishes 'stable coin' guidelines" (11 September 2019) (last visited 13 July 2020), online: *FINMA* <www.finma.ch/en/news/2019/09/20190911-mm-stable-coins>.

134 David Pan, "China's Crypto Czar: Facebook-Led Libra 'Might be Unstoppable'" (19 September 2019) (last visited 13 July 2020), online: *CoinDesk* <www.coindesk.com/chinese-crypto-czar-no-one-would-say-welcome-to-libra-but-it-might-be-unstoppable>.

135 Frank Tang, "Facebook's Libra forcing China to step up plans for its own cryptocurrency, says central bank official" (8 July 2019) (last visited 13 July 2020), online: *South China Morning Post* <www.scmp.com/economy/china-economy/article/3017716/facebooks-libra-forcing-china-step-plans-its-own>.

fluctuation and deviation from the existing banking system.[136] It is implicit in his message that the DCEP has nicely patched up all these loopholes present in Libra.

4. STRUCTURAL DESIGN OF THE DCEP AND SAFEGUARDS AGAINST RISKS

The key features of the DCEP system can be summarized in "One Currency, Two Vaults, Three Centres."[137] The first vault is the DCEP Issuance Vault, which takes the form of a private data cloud managed by the PBOC where the database for the issuance of DCEP is stored. The second vault is the DCEP Commercial Banks Vault, where commercial banks similarly have their own clouds to store the encrypted data strings representing the DCEP. The role of commercial banks, while possibly weakened, is nevertheless not entirely diminished with the introduction of the DCEP. The "Central Bank — Commercial Banks binary" is still kept where the Central Bank is responsible for the issuance, verification and monitoring of the DCEP, and the commercial banks are responsible for offering services for the circulation and construction of an application ecosystem of the DCEP by directly interacting with the general public.[138]

The three centres would be the Registration Centre, the Verification Centre and the Big Data Analysis Centre. The Registration Centre registers the ownership of the DCEP and records the corresponding owner's identity. It also records the whole process of creation, circulation, inventory verification and destruction of the DCEP. The Verification Centre performs centralized management of the identity information of DCEP-related institutions and users. It is a basic component of the system's security and an important link in the controllable design of anonymity. Lastly, the Big Data Analysis Centre is responsible for AML operations, payment behaviour analysis and the oversight and adjustment of key parameters.

On the user end, each user has a DCEP digital wallet installed in the form of either hardware or software. The security chip in the user terminals is the medium in which the integrity of the private keys and the algorithmic process is further protected. The following discussion highlights mechanisms to guard against potential risks.

---

[136] Zhou Yanyan, "Huángqífān: Zhōngguó yāngháng hěn kěnéng zài quánqiú dì yī gè tuīchū shùzì huòbì" [Huang Qifan: China's Central Bank will be the First in the World to Roll Out Digital Currency] (28 October 2019) (last visited 13 July 2020), online: *21st Century Finance* <m.21jingji.com/article/20191028/herald/433482a2c9b6d35c1d2e3cdf7977244d.html>.

[137] Qian Conceptual Prototype, *supra* note 14. See a diagram of the structural illustration of the DCEP at 14.

[138] *Ibid.*

(a) Cryptography to Enhance Security

As previously mentioned, the DCEP is considered by the PBOC to be a cryptocurrency in the technical aspect and leverages cryptographic technology for its security and credibility.[139] The design of the DCEP presentation format will be protected by cryptography, allowing it to be circulated and stored without being forged, duplicated, double-spent or rejected, thus mitigating the concern over digital forgery and alteration.[140] On the P2P level, the techniques of cryptography, blockchain and DLT, trusted cloud computing and Secure Element are utilized to make sure the DCEP cannot be stolen, tampered or duplicated in P2P transfers.[141] Specific cryptographic technology such as the Hash functions, Fitzer algorithm, blind signature and ring signature may also be used to further encrypt the data string representing the DCEP and safeguard its security.[142]

However, the use of cryptography does not suggest that the DCEP is 100% free from hacking. Many of the above-mentioned concepts are still at the theoretical stage, and it remains to be seen how they can integrate with the system or whether there will be other forms of weakness in the design. The high-level concentration of DCEP codes with the three centres managed by the PBOC would also make them more susceptible to attacks. This article does not make a definitive conclusion on this point as much is to be determined by computer science experts, the scenarios revealed by the pilot runs and actual implementation.

(b) Striking the Right Balance: "Voluntary Anonymity at Front End and Real-Name at Back End"

As above-mentioned, it is an intentional choice of design whether the DCEP wants to adopt anonymity or the real-name system. The PBOC has chosen the intermediary approach of "Voluntary Anonymity at Front End and Real-Name at Bank End."[143] This means that at the front end, users can choose to remain anonymous while security and data protection technologies will be used to block out unauthorized access of user data. At the back end, experts in the PBOC are nevertheless able to track down the parties behind a certain transaction and make use of the RegTech developed at the Big Data Analysis Centre to combat illegal transactions, money-laundering, terrorist financing and tax evasion.[144] Hence, this front end-back end dichotomy attempts to strike a balance between safeguarding user's personal information and combating illegal activities.

---

[139] Qian Systematic Framework, *supra* note 5.

[140] *Ibid.*

[141] Yao Qian & Tang Yingwei, "Guānyú yāngháng fādìng shùzì huòbì de ruògān sīkǎo" [Several Thoughts on Central Bank Digital Currency] (2017) 7 Finance Res at 78-85.

[142] *Ibid.*

[143] Qian Conceptual Prototype, *supra* note 14.

[144] Qian Systematic Framework, *supra* note 5.

On top of the benefits of traceability provided by the back-stage real-name system, the DCEP is inherently more firmly fortressed against the funding of illegal activities because of the supervision by a third-party Central Bank throughout the lifecycle of the DCEP and the lack of vulnerabilities inherent in decentralized cryptocurrencies such as Bitcoin, including the 51% attack and the Goldfinger attack, where a theoretical majority holder of 51% of Bitcoins could dictate the rules in a malicious manner.[145]

Nevertheless, the concept of "Voluntary Anonymity at Front End and Real-Name at Bank End" is still in its draft form, and much clarity is desired in terms of where the line is drawn between the front end and the back end. Furthermore, it remains to be tested whether the back end servers are as impenetrable as claimed and whether there can actually be leakage of information from the back end as well. For instance, independent contractors collaborating with the PBOC to facilitate the work of the three centres have access to "back end" information but may be more vulnerable to attacks or bribes to leak out information.

(c) Compatibility with the Current Market Structure

Unlike Bitcoin and Libra, which are positioned to disrupt the current market structure and monetary system, the DCEP has deliberately chosen structural designs to be compatible with and facilitate the current market structure. As both the Deputy Director of the PBOC, Fan Yifei, and Chairman of the PBOC Digital Currency Research Institute, Mu Changchun, have repeatedly emphasized in their public speeches, the DCEP system will consistently adopt the *"two-tier" system* (i.e., keeping the Central Bank — Commercial Bank binary) and centralized management in order to best integrate with the existing market structure.[146]

In maintaining the "two-tier" Central Bank — Commercial Bank binary, the PBOC seeks to utilize the resources, talents and existing IT infrastructure of the commercial banks. This arrangement also facilitates risk minimization and management. It would be almost inconceivable for the PBOC alone to deal with the tremendous volumes of transactions entered into every second by billions of Chinese users with vastly different needs, intentions, education level and technical savviness. It would instead be much more comfortable for the commercial banks to retain and deal with their old customers. Most importantly, the two-tier structure prevents "financial disintermediation,"

---

[145] Trautman, *supra* note 67.

[146] Mu Changchun, "Zhōngguó yāngháng shùzì huòbì cǎiqǔ shuāng céng yùnyíng tǐxì, zhùzhòng M0 tìdài" [China's DCEP Adopts Two-Tier Operation System, and Focuses on Replacing M0] (10 August 2019) (last visited 13 July 2020), online: *Sina* <finance.sina.cn/forex/hsxw/2019-08-21/detail-ihytcern2373190.d.html>; Fan Yifei, "Guānyú yāngháng shùzì huòbì de jǐ diǎn kǎolü" [Several Thoughts on the DCEP] (25 January 2018) (last visited 13 July 2020), online: *YICAI* <www.yicai.com/news/5395409.html>.

which happens when customers switch from commercial banks to the Central Bank, causing significant disruption to the existing monetary system.[147]

Furthermore, by insisting on a centralized management of the DCEP, the PBOC is able to maintain or even enhance its control over monetary policy on the macroeconomic level, as discussed in Section III.B, prevent over-issuance of the DCEP and associated inflation and keep public trust and confidence in a stable value of the DCEP backed by sovereign credit. By implementing these structural designs, the PBOC is making sure there is a minimum shock to the consumers on the user level and the commercial banks on the intermediary level when the DCEP is introduced.

Table 1 below presents a summary of the key differences between the DCEP, Bitcoin and Libra based on the above discussion. It can be seen from the Table that while Facebook's Libra is able to tackle some of the fatal flaws in Bitcoin's design, such as low transaction volume and high-value fluctuation, it still falls short of adequately dealing with the risks of condoning illegal activities and leakage of personal data. The DCEP, on the other hand, has proposed some structural safeguards against these risks, while their effectiveness remains to be tested.

Table 1: A Table of Comparison between the DCEP, Bitcoin and Libra

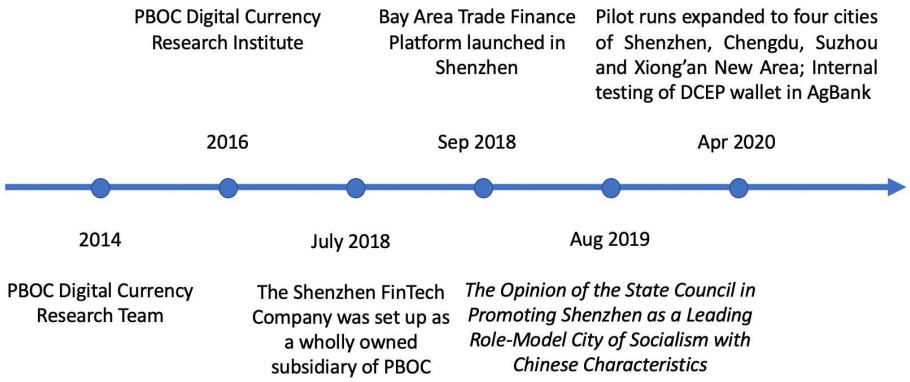
	Bitcoin	Libra	DCEP
Acceptance by User	Low	Potentially High	Potentially High
Legal Tender	No	No	Yes
Whether Centralized	Decentralized	*De facto* centralized	Centralized
Transaction Volume	7 / second	1,000 / second	Higher than 1,000 / second
Transaction Speed	Low	High	High
Transaction Cost	Some	Low	Low
Risk of Duplicability and Counterfeit	Low	Low	Low
Anonymity or Real Name	Anonymous	Anonymous	"Voluntary Anonymity at Front End; Real-Name at Back End"
Personal Data Protection	High	Questionable	High
Risk of Illegal Activities	High	High	Low
Value Fluctuation	Extreme (speculations & expectations)	Low (backed by a reserve of assets/currencies)	Zero (fixed value)
Effect on Monetary Policy	Disruptive	Disruptive	Facilitative
Disruption to Commercial Banks	High	High	Low, "two-tiered system"

147 *Ibid.*

(d) Incremental Approach: The Pilot Runs

Being one of the four Special Economic Zones set up in the 1980s and probably the most economically vibrant, technologically innovative and internationally recognized one after decades of development,[148] Shenzhen is chosen as the ideal testbed for a trial run and further development of the DCEP system. Figure 1 below presents a timeline of key milestones in the development of the DCEP.

Figure 1: A Timeline of Key Milestones for the DCEP



In July 2018, the PBOC set up a new 100% owned subsidiary, the Shenzhen FinTech Company, and the Company's stated objectives include FinTech-related technology development, with a focus on blockchain, as well as technology consulting, transfer, operation and maintenance.[149]

On 4 September 2018, with the support of the PBOC, the PBOC Digital Currency Research Institute, and other prominent commercial banks such as the Bank of China, China Construction Bank and Standard Chartered, the Shenzhen FinTech Company launched the Bay Area Trade Finance Platform.[150] As its name suggests, the Bay Area Trade Finance Platform targets the Guangdong,

---

[148] China, State Council, *The Opinion of the State Council in Promoting Shenzhen as the Leading Role-Model City of Socialism with Chinese Characteristics*, (State Council, 9 August 2019) [*Shenzhen as the Leading Role-Model City*].

[149] Sina Finance, "Yǒu guānfāng bèijǐng de shēnzhèn jīnróng kējì yǒuxiàn gōngsī, jiāng zěnme wán qū kuài liàn" [Backed by Official Support, How Will the Shenzhen FinTech Company Develop Blockchain?] (6 September 2018) (last visited 13 July 2020), online: *Sina Finance* < cj.sina.com.cn/articles/view/1663315964/63242ffc02700afjk > .

[150] Mars Finance, "Jiěmì yāngháng qíxià qū kuài liàn gōngsī: Qùnián cheng lì, céng 10 wàn yuèxīn zhāopìn qū kuài liàn jiàgòu shī" [Decrypt the Blockchain Company of the Central Bank: Formed Last Year, and Once Recruited a Blockchain Architect with a Monthly Salary of ¥100000] (8 August 2019) (last visited 13 July 2020), online: *ChainNews* < www.chainnews.com/articles/392680500179.htm > .

Hong Kong and Macau areas (also known as the "Greater Bay Areas"),[151] setting its long-term vision on developing a national or even global open trade and finance ecosystem.[152]

Phase one of the Platform established the fundamental layer of a trade and finance platform based on blockchain technology, on which, various trade and finance activities, including handling accounts receivables and conducting trade financing, can take place. More importantly, the Platform provides an entire trade and finance inspection and regulation system, allowing the regulators to perform dynamic real-time monitoring and regulation of financial activities.[153] During the 2019 China International Big Data Expo, Deputy Director of the PBOC Digital Currency Research Institute, Di Gang, announced that the Platform had developed four apps, collaborated with 26 banks and completed more than 17,000 transactions with the transaction value exceeding four billion RMB.[154]

On 9 August 2019, the State Council issued *The Opinion of the State Council in Promoting Shenzhen as the Leading Role-Model City of Socialism with Chinese Characteristics*, and at § 2.5, expressly mentioned its support for Shenzhen to: "[D]evelop digital economy innovation and development experimental zone; *carry out research on digital currency and mobile payment*; take advance steps on expanding the internationalization of the RMB and explore transboundary financial regulations."[155]

Hence, the *Opinion* officialized the role of Shenzhen as a testbed for the rolling out of the DCEP and its supporting digital structures. It is submitted that such is a prudent and incremental approach. By using Shenzhen as a testbed, the PBOC is able to collect valuable data on the key parameters surrounding the DCEP, including its acceptance rate, usability, scalability, as well as how can commercial banks and financial institutions facilitate its roll-out and benefit from its development. Most importantly, it allows the PBOC to minimize risk and conduct damage control should any of the above-mentioned fault-lines and legal implications materialize during the trial run.

Following Shenzhen, in April 2020, the pilot run for the DCEP was expanded to a total of four aspiring cities of Shenzhen, Suzhou, Chengdu and Xiong'an New Area.[156] At the same time, the Agricultural Bank of China

---

[151] Nicky Morris, "China's Central Bank Blockchain Trade Finance Initiative" (2018) (last visited 13 July 2020), online: *Ledger Insights* < www.ledgerinsights.com/chinas-central-bank-blockchain-trade-finance/ > .

[152] *Ibid.*

[153] *Ibid.*

[154] Mars Finance, "Yāngháng shùzì huòbì yánjiū suǒ fù suǒ cháng dí gāng: Yāngháng yǐjīng zài shìdiǎn màoyì jīnróng qū kuài liàn píngtái" [Deputy Director of the PBOC Digital Currency Research Institute Di Gang Pronounced PBOC's Trial Run on the Trade and Finance Blockchain Platform] (27 May 2019) (last visited 13 July 2020), online: *Mars Finance* < news.huoxing24.com/20190527103119674832.html > .

[155] *Shenzhen as the Leading Role-Model City*, *supra* note 148, § 2.5.

(AgBank) started internal testing of the DCEP wallet.[157] By this time, a total of 84 intellectual properties have been registered for the DCEP system.[158] Going forward, it is not sufficient to just announce the pilot runs but also be as transparent as possible in sharing the loopholes exposed by the pilot runs and their implications on the practicability of the DCEP.

5. STEPS FORWARD TO CONSTRUCT LEGAL FRAMEWORK AND BUTTRESS SECURITY

The structural design of the DCEP shows promise in tackling the legal issues identified. However, there is still a certain gap between the theoretical sketch of the DCEP and the practical difficulty and complexity of these issues. For instance, future advances in cryptography and computer science could add new areas of vulnerabilities to the digital foundation of the DCEP. Novel issues could also emerge in transaction scenarios of which the designers may not have thought and, therefore, posing challenges to judges in settling disputes. This article, therefore, makes the following recommendations aimed at the construction of a legal framework surrounding the DCEP and strengthening protection against earlier identified risks of cyber attack, leakage of personal information and money-laundering.

(a) Update and Revision of Legal Concepts

While it is fundamental to overcome the technological hurdles for the DCEP, it is equally important for relevant legal definitions to be updated to accommodate the DCEP. Such legislative amendments cannot lag behind the development of the DCEP, and judges must be equipped with an appropriate legal lexicon to deal with potential future disputes concerning the DCEP.

To begin with, the current definition of RMB, which only covers physical banknotes and coins under § 2 of the *RMB Rules*,[159] has to be expanded to include the DCEP, thereby conferring the recognition of the DCEP as a legal tender. Additionally, the current legal definition of forgery or alteration has to be updated as well. According to the *2003 PBOC Regulations on the Identification and Confiscation of Counterfeit Money*,[160] and the *2010 Supreme People's Court's Interpretation on Several Issues Concerning the Specific Application of Law in the*

---

[156] Xinhua, "Yãngháng: Shùzì rénmínbì zhèngzài sì de nèi cè" [Central Bank: Piloting of the DCEP in 4 Cities] (20 April 2020) (last visited 13 July 2020), online: *Xinhua* < www.xinhuanet.com/fortune/2020-04/20/c_1125878094.htm > .

[157] Sina, "Zhòng bàng! Yãngháng shùzì huòbì DCEP zài nóngxíng nèi cè" [Breaking News! Internal Testing of the DCEP at Agricultural Bank of China] (15 April 2020) (last visited 13 July 2020), online: *Sina Finance* < finance.sina.com.cn/blockchain/roll/2020-04-15/doc-iirczymi6410219.shtml > .

[158] ChainNews, "Zhõngguó wèi yãngháng shùzì huòbì shẽnqĩng 84 xiàng zhuãnlì" [China Registers 84 Intellectual Properties for the DCEP] (13 February 2020) (last visited 13 July 2020), online: *ChainNews* < www.chainnews.com/articles/849026539038.htm > .

[159] *RMB Rules*, *supra* note 33.

Trial of Cases of Counterfeiting Currency (Vol. 2),[161] "forgery" is defined as "the act of making counterfeit currency and posing as real currency, *imitating the pattern, shape, colour, etc. of real currency*," and "alteration" is defined as "the act of changing the form and value of real currency via *techniques such as cutting and pasting, de-layering and reprinting, etc*." Such definitions would be inapplicable to the crime of counterfeiting DCEP, which is, in essence, a string of encrypted numbers without a physical form. Accordingly, it is recommended that the definition of forgery be expanded to include any unauthorized creation of data representing the DCEP. The definition of alteration should also be expanded to include any unauthorized manipulation of the DCEP data created and distributed by the PBOC.[162] Along the same vein, the relevant definitions in a series of legislations, including the *PBOC Law, Anti-Money-Laundering Law*, Book Two of the *PRC Civil Code* on property rights[163] and the *Personal Information Protection Law* currently being drafted, all need to be amended accordingly.

(b) Role of PBOC Re-Examined

Under the current mandate stipulated by the *PBOC Law*, the role of PBOC includes; "1) design and implement monetary policy; 2) issue and manage the circulation of the RMB; 3) authorize, supervise and regulate financial institutions; 4) regulate financial market," among other duties.[164] With the introduction of the DCEP, it is foreseeable that the role of the PBOC would expand extensively into new areas that were not previously under its purview. These new areas would include issuance and management of account data of the DCEP, development and administration of the DCEP system, agreement with partners and contractors, transaction authorization, system security against cyber attack and fraud and interoperability with other existing infrastructure.[165] AML obligations that previously mainly rested on financial institutions, in accordance with *Anti-Money-Laundering Law*,[166] now need to be applied to PBOC as well. The extent of the applications would depend on how much interaction PBOC has with DCEP account holders in account opening and monitoring of transaction data.

---

[160] *PBOC Regulations on the Identification and Confiscation of Counterfeit Money ( ), People's Bank of China, 2003*.

[161] *Supreme People's Court's Interpretation on Several Issues Concerning the Specific Application of Law in the Trial of Cases of Counterfeiting Currency (Vol. 2)*), Supreme People's Court, 2010.

[162] Liu Legal Issues, *supra* note 34.

[163] *PRC Civil Code*, National People's Congress, 2020, Book II, "Property Rights".

[164] *PBOC Law*, *supra* note 35, § 4.

[165] See for reference, the anticipated role of the Central Bank explained in Riksbank 1, *supra* note 12 at 23.

[166] *PRC Anti-Money-Laundering Law, supra* note 68, Chapter III, "Anti-Money-Laundering Obligations of Financial Institutions".

Such drastic changes would mean significant organizational and manpower challenges for the PBOC, as the PBOC would share some of the responsibility of the commercial banks in the management and monitoring of millions of DCEP accounts. Accordingly, the government should explain how the PBOC plans to deal with these challenges. What are the new operational and supervisory departments to be established? A crucial question is will all these functions will be conducted by the PBOC internally or will there will be outsourcing to third-party service providers? In the latter scenario, it is crucial to explain and assess the identity or selection process for these service providers and the mechanisms in place to ensure their integrity and security.

(c) Strengthening Personal Data Protection Regime

As previously mentioned, the *PRC Personal Data Protection Law* is still in the process of drafting. Nevertheless, there are a number of brief provisions covering personal data protection in the *PRC Civil Code*. Under Book I, "General Principles," Chapter V, "Civil Rights," § 111 stipulates that:

> [T]he personal information of a natural person shall be protected by law. Any organization or individual needing to obtain the personal information of other persons shall legally obtain and ensure the security of such information, and shall not illegally collect, use, process, or transmit the personal information of other persons, nor illegally buy, sell, provide, or publish the personal information of other persons.[167]

More detailed provisions are found in Book IV, "Personality Rights," Chapter VI, "Right of Privacy and Protection of Personal Information." Section 1034 reiterates that personal information is protected, gives a definition and highlights a few important categories.[168] Subsequent sections state the principles of legality, appropriateness and necessity in the collection of personal information, the avoidance of excessive collection and processing and that the collection should be in accordance with laws and regulations, given consent of the individual while providing open disclosure of the purpose, method, and rules of collection.[169] Information collectors should take relevant precautions, technological or otherwise, to protect personal information, prevent leakage or manipulation and report and recover in case of leakage.[170] State organs are bound by confidentiality obligations concerning the personal information they collected.[171] The 9th amendment of the *PRC Criminal Law*, in 2015, made it a criminal offence to illegally obtain, provide or sell personal information, with

---

[167] *PRC Civil Code*, *supra* note 163, § 111.

[168] *Ibid.*, Book IV, Chapter VI, § 1034.

[169] *Ibid.*, § 1035.

[170] *Ibid.*, § 1038.

[171] *Ibid.*, § 1039.

fines and sentencing of three years and below for serious offences, and three to seven years for exceedingly serious offences.[172]

However, gaps remain in the above-mentioned limited number of provisions with vague wordings. For instance, there is insufficient guidance to key phrases such as "appropriateness and necessity," "excessive collection," "relevant precautions" and "exceedingly serious offences," leaving much grey area for the implementation of the rules. In this regard, much can be learned from foreign jurisdictions with extensive personal data protection laws[173] Take the European *General Data Protection Regulation* for reference, where rights of data subjects and the obligations of data controllers and processors are very clearly set out.[174] Important rights of the data subjects include the right to be fully informed of the details of the collection and processing of data.[175] These details include contact details of the controller, the purpose and legal basis for the processing, the recipients of the data and whether there is any transfer to a third country or international organization. Data subjects should also be able to retain the right to access,[176] rectify,[177] request the erasure[178] or restrict the processing of data,[179] including any automated decision-making.[180] The data subjects have to be informed of all these rights at the point of data collection,[181] and any request must be processed within 30 days.[182]

Correspondingly, the obligations of the data controllers entail the implementation of appropriate technical and organizational measures to ensure security, including *inter alia*, pseudonymization and encryption, confidentiality measures, recovery measures in the event of an incident and regular testing and assessment.[183] Data protection impact assessments are required for processing involving high risk, new technology or special categories of data.[184] Controllers should only engage data processors on a contractual or otherwise legal basis and ensure the processors fulfill similar obligations.[185] The

---

[172] *PRC Criminal Law*, National People's Congress, 1979, § 253.

[173] Huaiyin, *supra* note 56.

[174] *General Data Protection Regulation*, *supra* note 51, Chapter 3, "Rights of the Data Subject"; Chapter 4, "Controller and Processor".

[175] *Ibid*., § 13, "Information to be provided where personal data are collected from the data subject".

[176] *Ibid*., § 15, "Right of access by the data subject".

[177] *Ibid*., § 16, "Right to rectification".

[178] *Ibid*., § 17, "Right to erasure".

[179] *Ibid*., § 18, "Right to restriction of processing".

[180] *Ibid*., § 22, "Automated individual decision-making, including profiling".

[181] *Ibid*., § 13(2).

[182] *Ibid*., § 12(3).

[183] *Ibid*., § 32, "Security of processing".

[184] *Ibid*., § 35, "Data protection impact assessment".

[185] *Ibid*., § 28, "Processor".

Regulation encouraged the setup of supervisory bodies to implement a set of code of conducts[186] and certification mechanisms,[187] which can help to demonstrate the controller's compliance with obligations.

Other advanced economies have also set up extensive personal data protection laws of a similar nature. Japan implemented the *Act on the Protection of Personal Information* in 2003,[188] while Singapore enacted the *Personal Data Protection Act* in 2012.[189] The Chinese government can do well to study the provisions of these data protection laws and selectively adopt the parts that fill the existing gaps and ambiguity in Chinese law. This process is of crucial importance with the introduction of the DCEP, which would create an unprecedented congregation of personal information, transactional history and digital money. When using the DCEP, consumers must be reassured by appropriate data protection laws that their private information would not be used against them by malicious parties, allowing them to claim for damages in court should leakages occur.

(d) Appropriate Reporting on Cyber Resilience Framework

Given the risk of cyber attacks on the DCEP and its serious repercussions, the PBOC should implement a holistic cyber-resilience framework and make an appropriate public announcement of such a framework. Insights on such a framework can be gleaned from guidelines released by international organizations like the IMF,[190]the BIS[191] and the World Bank.[192] Take the *Guidance on Cyber Resilience for Financial Market Infrastructures* published by the BIS, for example. A cyber-resilience framework should articulate a system's cyber-resilience objectives and cyber risk tolerance by elaborating on the key components of "(i) governance; (ii) identification; (iii) protection (iv) detection; and (v) response and recovery," together with the overarching components of "(i) testing; (ii) situational awareness; and (iii) learning and evolving."[193] Of

---

[186] *Ibid*., § 40, "Code of conduct", § 41, "Monitoring of approved codes of conduct".

[187] *Ibid*., § 42, "Certification", § 43, "Certification bodies".

[188] *Act on the Protection of Personal Information*, *2003*, No. 57.

[189] *Personal Data Protection Act, 2012*, No. 26.

[190] Tamas Gaidosch et al., "Cybersecurity Risk Supervision" (2019) Departmental Paper No.19/15 (last visited 13 July 2020), online: *IMF* <www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/23/Cybersecurity-Risk-Supervision-46238>.

[191] Bank for International Settlements, "Guidance on Cyber Resilience for Financial Market Infrastructures" (2016) (last visited 13 July 2020), online (pdf): *BIS* <www.bis.org/cpmi/publ/d146.pdf> [BIS Guidance on Cyber Resilience].

[192] Aquiles A. Almansi, *Financial Sector's Cybersecurity: Regulations and Supervision* (Washington: The World Bank Group, 2018), online (pdf): *World Bank* <documents1.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf>.

[193] BIS Guidance on Cyber Resilience, *supra* note 191, § 1.2.

particular relevance to the DCEP is the advice that protection should not only guard against external threats but also insider threats by paying attention to the training of personnel with high-level access and potentially low tech-savviness.[194] The financial infrastructure should also conduct testing in the forms of vulnerability assessments, scenario-based testing, penetration tests and tests using red teams.[195] Equally important is the system's ability to gather intelligence about the cyber risks present in the environment it operates in,[196] while also learning and evolving with the advance of computer science.[197]

All this advice on constructing a cyber-resilience framework is highly instrumental for the implementation of the DCEP. The PBOC can use their above-mentioned pilot runs as a good basis to develop such a framework and report on its effectiveness. It is, therefore, suggested that the government should consider publishing an official report on the cyber-resilience framework they adopt for the PBOC, together with the invaluable insights and observations they made during these pilot runs. The content of the report could include the following sections. First, the scale of the pilot run, who are the participating merchants and banks, and how many users experienced the DCEP. Second, the functionality of the DCEP in terms of maximum transaction volume, transaction speed and accuracy levels. Third, any problem, improvement or troubleshooting concerning key components of the cyber-resilience framework. Fourth, feedback from major partners like commercial banks or major e-commerce giants like Alibaba or Taobao. By providing an adequate level of disclosure in these areas, the government will be able to harvest more help from a broad range of experts and academics in scrutinizing and improving the project and also build confidence among the public on an informed basis.

(e) Individual Amendments or the PRC DCEP Law

There are two possible ways to implement the above-mentioned recommendations, either through legislative amendment of a number of legislations identified above or through the introduction of a new piece of *PRC Digital Currency Electronic Payments Law* covering all these issues in the context of the DCEP. While individual amendment of each legislation may be a neater solution, such a process is exceedingly time-consuming. It has hardly been the case for the legislature to introduce an amendment just to change one definition. Therefore, it is also conceivable to have a stand-alone *PRC Digital Currency Electronic Payments Law* covering all these issues and other DCEP-specific legal issues in one piece of legislation.

Although such legislation has not been officially stated, it has been proposed by scholars such as Liu Xiangmin, Director of the Law & Regulations

---

[194] *Ibid*., §§ 4.4, 4.5.

[195] *Ibid*., § 7.2.2.

[196] *Ibid*., § 8.2.2.

[197] *Ibid*., § 9.

Department of PBOC.[198] It is suggested that this law should govern all aspects of the DCEP not already covered by other legislation with the aim of providing greater clarity on the legal framework supporting the DCEP and guiding judges in adjudicating cases.

The key aspects of the *PRC Digital Currency Electronic Payments Law* should include, *inter alia*, 1) definitions, 2) licensing and registration of service providers, 3) obligations and prohibitions, 4) supervision and inspection by a regulatory body, 5) security and access of systems, 6) data protection and 7) accountability, liability and compensation. The legislation should spell out clearly what each level of the system, from the PBOC to commercial banks and third-party contractors (e.g., app developers) should and should not do. These responsibilities should include the design of the system, the registration and protection of customer information and the performance of reporting, auditing, AML and CTF obligations. Further, they should explain how these activities are supervised and governed by a specially designated regulatory body. This piece of legislation also needs to be very clear in drawing the boundaries of accountability and liability arising in novel scenarios pertaining to the use of the DCEP. For instance, who should bear the liability, and how should compensation be decided in the event of a cyber attack that results in the loss of the DCEP in the digital wallet or the digital vaults maintained by banks? Is there a mechanism to punish service providers who leaked customer information in order to deter future breaches? Such issues need to be carefully considered and provisionally taken care of by a piece of new legislation. Otherwise, the government risks losing public confidence and trust in the DCEP because if a major setback occurred, a considerable number of users would be left with no legal recourse for their losses.

6. CONCLUSION

This author ventures to suggest that a truly successful form of cryptocurrency would be one that merges and reconciles the technological process, functionality of the cryptocurrency, the needs of the financial and monetary system and relevant laws and regulations. While technological progress in blockchain and DLT has made the concept of a decentralized cryptocurrency such as Bitcoin possible for the first time, its spread is limited by practical constraints (see Table 1) such as high value fluctuation and low transaction volume, as well as its association with widespread criminal activities and violations of AML & CTF obligations. While Facebook's Libra has patched up some of the practical limitations of Bitcoin, it still has not provided a satisfactory answer to regulators on what mechanisms have been put in place for personal data protection or to combat illegal activities. This is especially so since the infamous Facebook data breach in 2019. In this regard, the design of the DCEP has proposed some answers to these concerns. Nevertheless, these proposals are still in draft form and, a great deal of more details are required to assess their

[198] Liu Legal Issues, *supra* note 34.

effectiveness. Much more insights are to be desired from the testing conducted in the pilot runs.

The assessment at this stage is that the DCEP is, on the one hand, attempting to take advantage of blockchain and cryptography technology for heightened security and non-temporality, and on the other, reaping benefits from its status as a CBDC and being recognized as a legal tender supported by sovereign credit. At the same time, the conscious design choices of the PBOC aim to achieve minimum disruption to the existing monetary system while positively promoting the effectiveness of monetary policies, in contrast to privately issued cryptocurrencies, who stand to challenge and weaken monetary policies. The DCEP also strives to strike an appropriate balance between anonymity and the real-name system in order to keep criminal activities at bay while safeguarding personal data.

The DCEP is definitely still a work in progress, and much needs to be done in constructing a legal framework and regulatory environment surrounding its introduction. The designers need to be responsive and ready to deal with new challenges arising from unexpected transaction scenarios and technical aspects. At this stage, it appears by the information released so far that the Chinese government is treating its DCEP with utmost seriousness and prudence. This article has also highlighted the promising features in its design. It leaves to be seen whether these mechanisms are truly effective in resolving the economic and legal issues they identified, whether loopholes and challenges will surface in the pilot runs and broader implementation and what the Chinese government's response will be in the face of these challenges.