Countermeasures against CBDC Financial Crimes

Tao Zhang[1*][0000-0003-1817-8379], Yitong Li[2][0000-0002-4096-3413]

[1]School of Computer, Nanjing University of Science and Technology Zijin College, Jiangsu, China
[2]College of Finance and Economic, Shandong University of Science and Technology, Tai'an, Shandong, China

[1]dypro_mike@outlook.com
[2]lincheng0731@gmail.com

Abstract. The traditional currency cross-border circulation model has many problems in terms of efficiency, cost, and security. The private digital currencies represented by Bitcoin and Ethereum are flourishing and occupying an increasingly important position in cross-border payments. However, digital currencies themselves face great uncertainty and affect the stable operation of the global monetary system. In response, countries have started to develop CBDCs to enhance their financial inclusion and international competitiveness of their currencies with the advantages of digital currencies. However, the birth of new technologies often creates new problems, and CBDCs face a trade-off between privacy and transparency in their design, which can directly affect the supervision of CBDC funds and lead to CBDCs becoming a tool for financial crimes. This paper introduces the background and dynamics of CBDC development and the challenges it faces and combines existing relevant research and literature to propose countermeasures against CBDC financial crimes from several aspects: big data, artificial intelligence, and new regulation. Finally, future research directions in this field are proposed.

Keywords: CBDC, Digital Currency, Financial Crime, AML, CTF

1 Introduction

Traditional cross-border currency movement models can be divided into three types: single platform model, interconnected model, and correspondent bank model. In practice for many years, the cross-border currency flow model centered on correspondent banking has shortcomings in terms of security, efficiency, and cost.

In addition to traditional monetary cross-circulation payment means, various private digital currencies are flourishing, occupying an increasingly important position in cross-border payments and potentially disrupting the traditional monetary system. Although digital currencies can overcome the defects of traditional currencies with the help of digital technology and form high-quality financial innovations, such innovations are disruptive. Specifically, digital currencies themselves face great uncertainty, affecting the operation of the global monetary system [1]. In the field of cross-border

H. Mallick et al. (Eds.): ICEMCI 2022, AEBMR 231, pp. 543–548, 2023.
https://doi.org/10.2991/978-94-6463-098-5_61

payments, while digital currencies serve as efficient and convenient payment tools, their anonymity also facilitates transnational money laundering and other crimes. Based on the perceived risk and value of private digital currencies, many countries have strengthened the regulation of digital currencies and have conducted studies on legal digital currencies and their cross-border flows. The independent or joint research and development of CBDC in each country is a response to the disorderly and unregulated development of private digital currencies and compliance with the digital currency innovation in the digital economy era. Compared with domestic circulation, CBDC cross-border flows face more obstacles due to issues such as monetary sovereignty, regulatory differences, and changes in the international monetary system, which also gives rise to a series of issues such as how to build a new international monetary system and payment infrastructure, how to construct new international monetary laws and how to regulate them. International organizations such as BIS and IMF, national central banks, and academics have conducted studies on CBDCs and their economic impact. The number of related studies has increased significantly in recent years.

This paper analyzes the background, dynamics, and challenges of the emerging CBDC. Chapter 2 will introduce the features and advantages of CBDCs and the trade-off between privacy and transparency with existing CBDC-related research and literature, pointing out that poorly designed and regulated CBDCs may become tools for transnational financial crimes. Chapters 3 and 4 give possible countermeasures against CBDC financial crimes from two aspects. Chapter 3 emphasizes the use of multi-channel data fusion combined with big data and artificial intelligence algorithms to detect suspicious CBDC transactions. Chapter 4 proposes the use of tiered CBDC accounts, the strengthening of cooperation and coordination mechanisms for cross-border transaction regulation, and the use of CBDC's innovative technologies to design new regulatory schemes to achieve "regulation by design" from the perspective of strengthening regulation. Chapter 5 concludes the paper and proposes future research directions.

2 Related work

“By the end of 2021, more than a quarter of central banks were developing or running CBDC pilots. To make sure that cross-border functionalities are considered in time, central banks across the globe must collaborate at an early stage. Only then can CBDCs have a significant impact on the costs, speed, access, and transparency of cross-border payments.”, said Skingsley, chair of the CPMI Future of Payments Working Group and First Deputy Governor of Sveriges Riksbank [2].

Some scholars believe that the research on CBDC is still in its infancy in most countries, and it is necessary to solve the following two basic questions before exploring the advantages of CBDC for cross-border flows. First, whether CBDC must adopt blockchain technology. The second is how CBDCs are issued and circulated [3].

Sriram Darbha and Rakesh Arora argue that, in general, lower levels of privacy protection are easier to achieve. For higher levels of privacy protection, the system must encapsulate the information in a reliable device. This increases complexity and raises

operational costs and computational expenses. As a result, there are significant challenges in scaling up to national population sizes, both with DLT and non-DLT platforms. Rushing to deploy the technology on a large scale, such as micro-payment systems applied to IoT terminals, will have unknown technical barriers that will lead to unpredictable risks [4].

Privacy protection and control of international monetary crime in CBDC cross-border flows are two sides of the same coin. On the one hand, when a country is concerned about privacy protection, it will tend to adopt a value-based CBDC scheme, the CBDC will exhibit anonymous cross-border circulation characteristics, which facilitates cross-border money transfer [5]. Therefore, value-based CBDCs may become a tool for money laundering and terrorist financing if they are not properly designed and regulated. Even if designers adopt account-based CBDC, users' personal information is only available to the central bank. This makes it more difficult to control currency crimes when countries are unable to collaborate throughout the regulatory process. This situation will get worse as the number of issuing countries increases.

3 Anti-CBDC financial crimes through risk detection algorithms

3.1 Strengthen the integration of multi-channel data

In addition to using data on the flow of funds between financial institutions and third-party payment platforms, regulatory institutes can also adopt a combination of data from government departments such as taxation, customs, transportation, courts, and multiple sources in the field of business activities. Through these channels, the sources of customer information are expanded, and the identification of suspicious transactions can be made more accurate and efficient by comparing customer information data.

After the data of large and suspicious fund transactions are reported to the AML center, the department forms the analysis report to be reviewed through data integration, information matching, and analysis. Based on the acquired information, the department will analyze the transaction situation and the relationship between transaction subjects. This makes it possible to trace the currency transaction, analyze the correlation, and seize suspicious currency when necessary.

3.2 Integration of existing big data and artificial intelligence solutions

The given table lists the related research into anti-financial crimes. These technologies have been partially implemented in traditional regulatory systems, which can also be modified to play an indispensable role in anti-CBDC financial crimes.

Table 1. Related Big Data and AI research (Self-generated)

Direction	Designers	Technology researched
Fraud detection	Yu et al.	Random wandering algorithm [6]
	Tran et al.	An improved system combining breadth-first search

		on the random wandering algorithm [7]
	Yang et al.	The search of suspicious nodes from known suspicious nodes [8]
Anti-money laundering	Sun et al.	Using complex network theory to study anti-money laundering [9]
	Liu et al.	Analysis of the fund flow relationship between money laundering linked accounts using topological institution analysis tools [10]
	Zhang et al.	Anti-money laundering system based on AI [11]

4 Anti-CBDC financial crimes through enhanced regulation

4.1 Anti-CBDC financial crimes by raising the entry threshold

Money laundering violations are often associated with major crimes such as economic crimes, drug transactions, and terrorist activities, and involve the financial sector. According to the characteristics of the CBDC system, hierarchical authorization can be considered. Digital wallets that store CBDC is reviewed by employing tiered authorization to better "know your customer" (KYC) and to set limits accordingly. If users only register their digital wallets through cell phone numbers, they can only meet basic needs such as small payments; if they need to obtain higher limits, they must further upload identification information.

4.2 Further strengthen cross-border transaction regulatory cooperation and coordination mechanism

Cross-border payment is an important application area of CBDC, involving regulatory synergy and mutual assistance among transnational and cross-regional. In regulatory practice, a multilateral regulatory cooperation mechanism should be actively prepared and established, and the "Group of 20" (G20) can be considered to take the lead in building a regulatory framework for CBDC cross-border payments; the IMF should take the lead in drafting multilateral regulatory rules, clarifying the rights and obligations of countries (regions) in the regulatory framework, and determining uniform standards and defining a unified standard and normative system, framework, as well as sorting out various financial risks and issuing risk guidelines. At the national (regional) level, the IMF should also actively explore bilateral and multilateral regulatory cooperation, clarify their respective jurisdictions, regularly conduct comprehensive research and cooperation, and consider establishing information and data sharing mechanisms for tax evasion, large suspicious transactions, money laundering, illegal financing, support for terrorist activities and other illegal and criminal acts that occur in the process of cross-border trade and payment settlement. Nations and regions shall actively explore cooperation mechanisms such as joint investigations and cross-border litigation.

4.3 New type of RegTech based on the new technology of CBDC

When it comes to anonymity, the trade-off between privacy and transparency will affect the effectiveness of the anti-financial crime crackdown. The emergence of CBDC allows the regulation to be embedded in the technology itself. Notably, design-based regulation has evolved from Lessig's "code is law" [12], which claims that behavior in cyberspace is controlled by software code. This concept has led to a new understanding of embedded regulation [13]. That is, regulation can be achieved proactively by dealing with the code itself [14]. The programmability presents multiple opportunities where AML based on embedded smart contracts and software can generate new crime prevention strategies, which is the so-called "regulation by design" [15]. Thus, this may address the issue of technical regulatory interoperability in the cross-border CBDC world. For instance, RegLang is a regulatory-oriented smart contract programming language that allows regulatory experts to write regulatory policies as digital regulatory rules and run them as smart contracts on the blockchain. If the transaction initiator or transfer recipient is on the blacklist, the transaction will be rejected by the supervisory contract [16].

5 Conclusion

As mentioned earlier, the emergence of CBDC can enhance financial inclusion and promote the regulation of funds. It will have a huge impact on the future global financial system and reshape the future of cross-border settlement business. The maintenance of monetary sovereignty by countries is an important driver of global competition for CBDC. However, CBDC still faces the contradiction of trade-off between privacy and transparency, and improper design and regulation may become a tool for cross-border financial crimes. Central banks and regulators should cooperate early on issues such as technical cooperation and joint monitoring of cross-border capital flows. There are many existing big data and artificial intelligence algorithms, but the application in the field of CBDC still lacks research and needs to be adapted to the details of the underlying system of CBDC in each country. At the same time, the new type of regulation based on CBDC smart contracts - "compliance into design" is also a key research direction for the future.

References

1. Gao Hongmin, Li Gang. Fintech, Digital Currency and the Restructuring of the Global Financial System[J]. Academic Forum, 2020, 43(2): 102-108. (In Chinese)
2. Carstens A. Digital currencies and the future of the monetary system[C]. Hoover Institution policy seminar. 2021, 89(1): 17.
3. Bu Xuemin. On the Challenges and Institutional Construction of Central Bank Digital Currencies' Cross-Border Flow[J]. Pacific Journal. 2021, 29(6): 25-38. (In Chinese)
4. Darbha S, Arora R. Privacy in CBDC technology[R]. Bank of Canada, 2020.

5. Wang Yuwei, Guo Shiping. The Challenges and the Risk Prevention of the Central Bank Digital Currency[J]. Journal of Yunnan University of Finance and Economics, 2020, 36(02): 12-18. DOI: 10.16537/j.cnki.jynufe.000542. (In Chinese)
6. Yu H, Kaminsky M, Gibbons P B, et al. Sybilguard: defending against sybil attacks via social networks[J]. IEEE/ACM Transactions on networking, 2008, 16(3): 576-589.
7. Tran N, Li J, Subramanian L, et al. Optimal sybil-resilient node admission control[C]//2011 Proceedings IEEE INFOCOM. IEEE, 2011: 3218-3226.
8. Yang C, Harkreader R, Zhang J, et al. Analyzing spammers' social networks for fun and profit: a case study of cyber criminal ecosystem on twitter[C]//Proceedings of the 21st international conference on World Wide Web. 2012: 71-80.
9. Sun Jing, Chen Qian, Wan Hong. Research on the identification of suspicious financial transactions based on complex networks[J]. Digital Technology & Application, 2013 (4): 206-207. DOI:10.19695/j.cnki.cn12-1369.2013.04.149. (In Chinese)
10. Sun Lifang, Tao Wenli, Chen Yanmiao. The use of topology tools in the analysis of financial flows in AML linked accounts[J]. Fujian Finance, 2013 (2): 39-45. (In Chinese)
11. Zhang Chenghu, Li Shi. Design of anti-money laundering system based on AI technology[J]. Financial Computer of China, 2005 (3): 44-47.
12. Lessig L. Code is law[J]. Harvard magazine, 2000, 1: 2000.
13. Zetzsche D A, Arner D W, Buckley R P. Decentralized finance[J]. Journal of Financial Regulation, 2020, 6(2): 172-203.
14. Nabilou H. Testing the waters of the Rubicon: the European Central Bank and central bank digital currencies[J]. Journal of Banking Regulation, 2020, 21(4): 299-314.
15. Torra V. Data privacy: foundations, new developments and the big data challenge[J]. 2017.
16. Gao Jianbo, Zhang Jiashuo, Li Qingshan, Chen Zhong. RegLang: A Smart Contract Programming Language for Regulation[J]. Computer Science, 49(6A): 462-468. DOI: 10.11896/jsjkx.210700016 (In Chinese)