Report Related to Crypto Money Laundering

Chunpeng Li, Wenhong Liu, Zhen Shen, Ning Xu and Zixiao Zhao

1 Introduction

With the rapid development of digital currencies, cryptocurrencies such as Bitcoin and Ethereum have occupied a significant position in the global financial market. As a disruptive financial technology, cryptocurrencies allow users to transfer value without disclosing any personal information. This anonymity and decentralization offer new avenues for criminals to engage in illegal activities. Therefore, traditional anti-money laundering (AML) mechanisms face unprecedented challenges. This paper aims to deeply analyze the role of cryptocurrencies in money laundering activities and the strategies adopted by different countries to address these challenges.

This paper first examines the diverse approaches to cryptocurrency money laundering issues globally, revealing the varying strategies of different countries in response to this emerging issue. Subsequently, the article details the specific methods of money laundering with cryptocurrencies and analyzes the effectiveness of existing AML measures.

Through these analyses, this paper aims to provide readers with an in-depth understanding of the issue of cryptocurrency money laundering and to propose effective suggestions and solutions for AML policies, aiding in more effective global responses to this challenge.

2 Differences between countries on cryptocurrency money laundering

At present, various countries mainly adopt the registration system. This requires users to require real-name authentication when exchanging fiat currencies and cryptocurrencies.

2.1 Countries that implement registration systems

These countries have corresponding controls on both natural persons and legal persons on this issue. It mainly includes registration, recording, identifying customer identities and notifications, etc. The main objects of control are virtual currency platforms operating in the country (regardless of whether the platform has an entity located in the country). This series of regulations also controls other transaction intermediaries in the country where they are located.

Among them, the Bank of Japan is relatively lax about identity checks. It was earlier requested by the FATF to strengthen countermeasures against money laundering[1]. This is mainly because people can open a bank account with a no-photo ID in Japan which increases the risk of

sending illegal funds through someone's account.

Japan began to gradually introduce registration regulations in 2017 to regulate intermediaries and platforms. And incorporate virtual currency transactions into existing laws on fund payments.

2.2 Countries to be registered

These countries are still torn between regulating cryptocurrencies and attracting investors. In particular, the United Kingdom reiterated its goal of becoming a global cryptocurrency centre in December 2022. However, fighting money laundering is still necessary in the view of these countries' governments. It will only be a matter of time before the registration system is implemented after many discussions.

2.3 Countries still under discussion

For various reasons, the governments of these countries had limited enforcement capabilities in the early stages of combating money laundering. However, because of fear of being evaluated as a high-risk money laundering country by international finance and international sanctions. These countries have already begun to take action against money laundering. But long-term plans are still being developed.

2.4 Countries that forbid cryptocurrencies

The characteristics of these countries are very different from the previous countries on the free flow of capital. They have all implemented partial or strict foreign exchange controls.

Mainland China made early attempts to regulate cryptocurrencies. However, most Chinese use cryptocurrencies to legally allow their funds to leave mainland China. Strictly speaking, they are not illegal gains. Since then, the mainland Chinese government realized that it is unable to effectively forbid capital outflows. Therefore, there is a blanket ban on cryptocurrencies due to their high risks.

"Virtual currency-related business activities are illegal financial activities," the People's Bank of China said, warning it "seriously endangers the safety of people's assets"[2].

3 Money Laundering

Methods of money laundering will be introduced by presenting a chart that illustrates the trend of key techniques employed in the money laundering process.

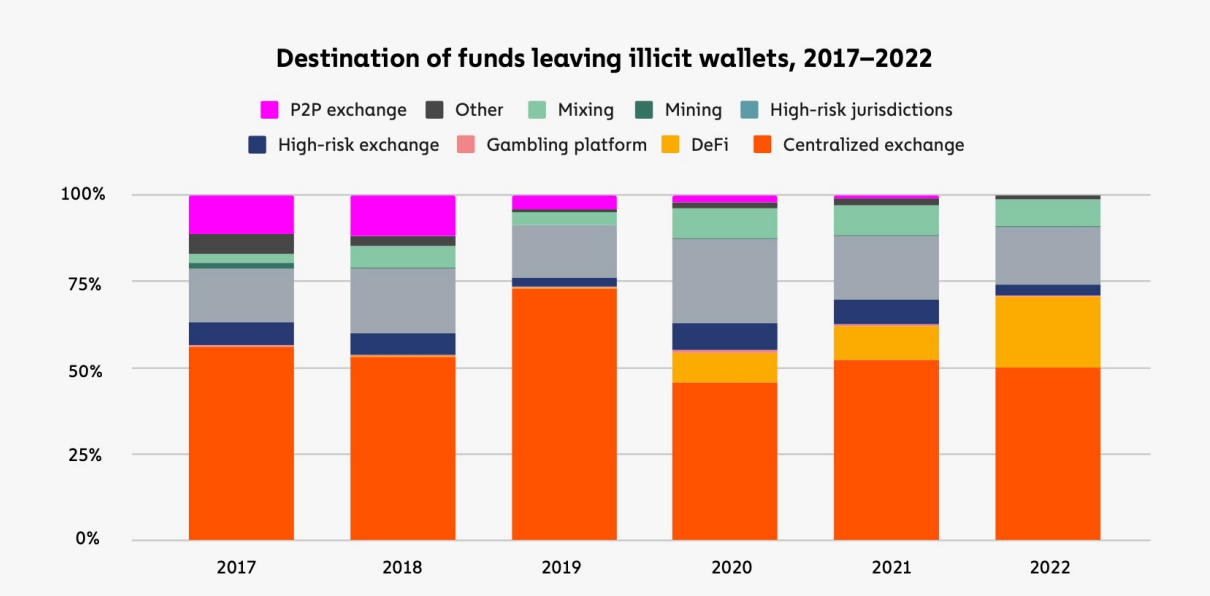

Figure 1: Destination of funds leaving illicit wallets [3]

Obviously, figure 1 illustrates that exchanges kept being the most popular destination of "Dirty money" which can be explained by "The goal of money laundering in cryptocurrency is to move funds to addresses where its original criminal source can't be detected, and eventually to a service that allows cryptocurrency to be exchanged for cash – usually this means exchanges."[3]

Centralised Exchanges, functioning as digital asset trading platforms, are overseen by a central entity, facilitating transactions. A potential method of money laundering involves the utilisation of "money mules" – individuals recruited to assist in transferring stolen money or conducting illegal financial transactions.

Criminals may directly or indirectly manipulate accounts created by money mules, transferring funds to external destinations like banks, as depicted in the accompanying figure 2.

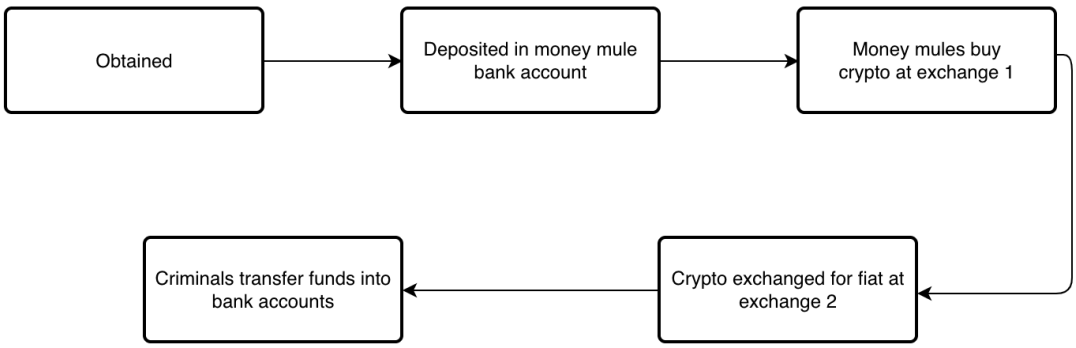

Figure 2: Flow of the dirty money

High-risk Exchanges, are exchanges that neglect regulatory and registration standards, allowing accounts established with minimal information. Criminals, utilising false details, exchange illicit crypto-assets for fiat currencies or other cryptocurrencies here, then withdraw the funds to a bank account or conceal the origin of the crypto-assets through diverse value transfer services. Another strategy involves transferring "clean" crypto-assets to reputable exchanges before cashing out, frequently converting transparent cryptocurrencies into privacy coins.

High-risk jurisdictions are regions susceptible to money laundering and terrorist financing, potentially facing international financial sanctions or appearing on the FATF's list of High Risk and Non-Cooperative Jurisdictions. Furthermore, countries with inadequate AML regulations or ineffective regulatory frameworks for crypto-assets are categorised as high risk. The money laundering methods of exchanges in these jurisdictions are similar to high-risk exchanges which discussed before.

Figure 1 illustrates the increasing prevalence of money laundering through decentralised finance (DeFi). Meanwhile, innovators have launched new DeFi applications based on smart contracts that can be used for lending, trading derivatives and other activities[4].

Among them, decentralised exchange services (DEX) are often used for money laundering activities. Due to imperfections in the regulations, it remains unclear whether DEX is an area of AML regulation, and know your customer (KYC) is usually not implemented, providing opportunities for criminals to launder money[5].

Simultaneously, real-time peer-to-peer swaps provide liquidity, allowing many kinds of tokens converted into bitcoin or ETH, facilitating access to cash. Additionally, mixers such as Tornado Cash are heavily used to conceal traces of illegal activity previously. The principle is that various entities deposit the crypto-asset into a mixer address as a pool, where anyone who deposited can generate a new address to withdraw the funds, making it impossible for a third party to find the link between the particular deposit address to a particular withdrawal address[6].

However, after Tornado was sanctioned, criminals turned to cross-chain bridges, this methodology same as the mixer, disrupting third-party tracing across the bridge and complicating the identification of the assets' original source[6, 7].

4 Anti-Money Laundering

Figure 3 elucidates the KYC process which is crucial in AML and combating illicit activities like the use of money mules.

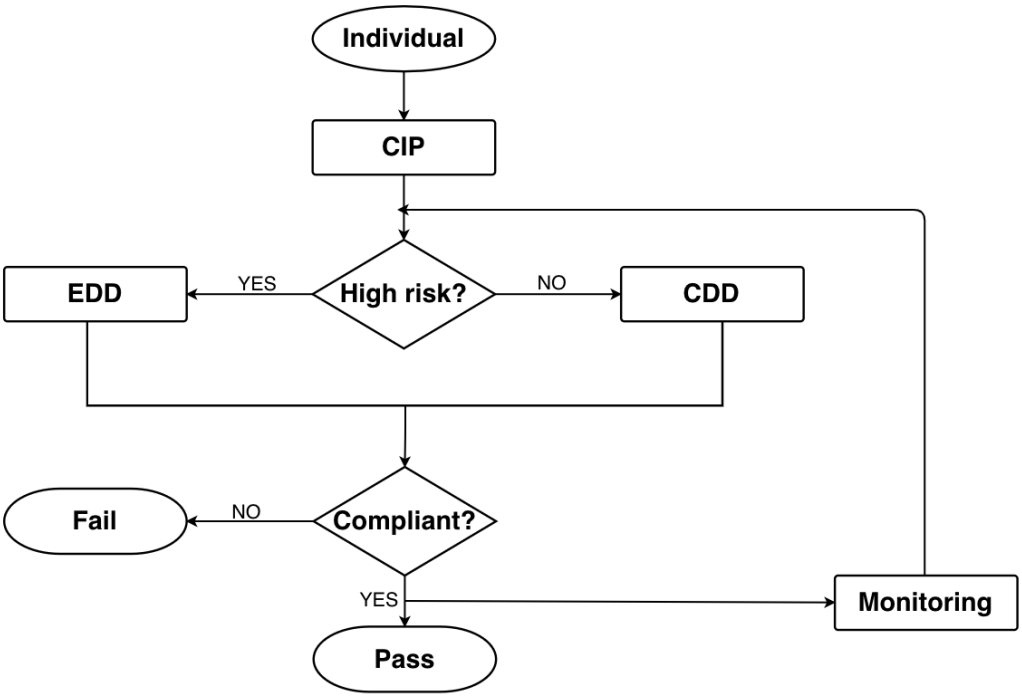

Figure 3: KYC strategy flow chart

The initial step of the KYC process involves a Client Identification Program (CIP) through either documentary or non-documentary methods, like cross-referencing with existing databases. This process aims to confirm the alignment of the client's fundamental details with their self-declared information and ensure they are not in the latest sanctions, watch lists, politically exposed person lists, or associated with high-risk regions.

Subsequent to the initial identification, the level of risk determines the application of Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD). This approach optimises resource efficiency and workload, effectively handling threats from criminal and terrorist activities. Due Diligence focuses on gathering additional customer information, identifying customer types, and aiding in detecting abnormal account transactions.

KYC-approved accounts undergo systematic monitoring, assessing transactions for unusual amounts, frequencies, locations, and other relevant indicators. The potential identification of suspicious activity may trigger the generation of Suspicious Activity Reports, enhancing overall market security.

In conjunction with the rigorous KYC processes that form the bedrock of financial integrity in the crypto space, the integration of traditional tools such as blacklisting emerges as a strategic measure to combat money laundering effectively.

The fundamental concept of blacklisting involves publicly marking specific addresses or crypto assets as "tainted"[8], effectively restricting their involvement in subsequent transactions. This approach aims to reduce the liquidity of identified illicit funds, by leveraging societal motivation

to reject flagged assets which is worthless.

The traditional method is tracking the origin of "dirty funds" entering the crypto network allows for the marking of the initial point as tainted, with the taint spreading as assets circulate. By tracing the taints, "dirty funds" can be frozen as long as they remain in the network. However, the successful implementation of this approach relies heavily on the efficiency of criminal investigations.

A possible alternate method is for exchanges to use machine learning-driven scrutiny and validate the transaction, assigning risk scores to transactions, requiring an explanation of high-risk transactions, and blacklisting those with high risks. Several companies like Elliptic are building large databases to map addresses to the holder to help realise this approach[9]. Challenges of this approach arise in maintaining accuracy and reliability. If a centralized agency was introduced for effective management, scrutiny, and complaint resolution, this would be a more powerful tool.

Though, the introduction of a centralised agency violates the principle of blockchain, striking a balance between effective AML measures and upholding decentralisation would help improve the circumstances of the crypto network.

However, both of these traditional approaches seem to be poorly adapted to the DeFi market. As previously mentioned, KYC is not effectively implemented in the DeFi market, where it is either entirely absent or voluntarily applied by projects. Additionally, regulators encounter challenges in categorizing various DeFi products and services, impacting the regulation and applicable rules[10].

The classification of DeFi, coupled with the establishment of relevant regulations and enforcement methods, should be promptly executed to address the current legislative gap. Currently, a practical approach to sanctioning illegal DeFi services involves discouraging their utilisation instead of complete usage restrictions since regulations cannot shut down smart contracts.

For instance, considering the case of Tornado Cash, regulators atook decisive action by shutting down the Tornado Cash website, which served as a user-friendly portal for accessing the mixing service. This move made it considerably more challenging for individuals to utilize the service. As a result, the user base significantly decreased, leading to a notable reduction in the inflow of crypto-assets. This, in turn, diminished the attractiveness of the platform for potential illicit activities by discouraging criminal engagement.

5 Conclusions and discussion

This paper points out that while cryptocurrencies have brought innovation to the financial markets, they have also posed significant challenges to existing anti-money laundering mechanisms. In addressing the issue of money laundering through cryptocurrencies, it is first necessary to recognize the technological risks involved: the anonymity and decentralization of cryptocurrencies provide concealed spaces for laundering activities. This urgently requires the development

of more precise technological tools, such as the use of artificial intelligence and machine learning technologies, to improve the efficiency of identifying and preventing suspicious activities. For instance, optimizing KYC (Know Your Customer) and AML (Anti-Money Laundering) strategies can lead cryptocurrency trading platforms to adopt more advanced customer identity verification and anti-money laundering control systems. Besides the technological risks, the inconsistency in global cryptocurrency regulatory standards provides opportunities for launderers. Therefore, strengthening international regulatory cooperation and unifying regulatory standards, including establishing global information-sharing mechanisms and coordinating cross-border regulatory frameworks, becomes crucial. Through globally coordinated efforts, we can not only ensure the safety and healthy development of the financial markets but also minimize the risks of money laundering and other related criminal activities to the greatest extent.

References

[1] M. Yamazaki and Y. Nitta, "Global watchdog urges japan to boost fight against money-laundering," Aug 2021. [Online]. Available: https://rb.gy/8maniu

[2] BBC News, "China declares all crypto-currency transactions illegal," Sep 2021. [Online]. Available: https://www.bbc.co.uk/news/technology-58678907

[3] T. Chainalysis, "The chainalysis 2023 crypto crime report," Feb 2023. [Online]. Available: https://go.chainalysis.com/2023-crypto-crime-report.html

[4] Elliptic, "Typologies report 2023," Dec 2023. [Online]. Available: https://www.elliptic.co/resources/elliptic-typologies-report-2023

[5] D. Dupuis and K. Gleason, "Money laundering with cryptocurrency: open doors and the regulatory dialectic," *Journal of Financial Crime*, vol. 28, no. 1, pp. 60–74, 2020.

[6] Elliptic, "The state of cross-chain crime report 2023," Dec 2023. [Online]. Available: https://www.elliptic.co/resources/state-of-cross-chain-crime-2023

[7] M. Nadler and F. Schär, "Tornado cash and blockchain privacy: A primer for economists and policymakers," *Available at SSRN 4352337*, 2023.

[8] K. Kolachala, E. Simsek, M. Ababneh, and R. Vishwanathan, "Sok: money laundering in cryptocurrencies," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 2021, pp. 1–10.

[9] M. Möser and A. Narayanan, "Effective cryptocurrency regulation through blacklisting," *Preprint*, 2019.

[10] V. Benson, U. Turksen, and B. Adamyk, "Dark side of decentralised finance: a call for enhanced aml regulation based on use cases of illicit activities," *Journal of Financial Regulation and Compliance*, 2023.