ISSN 2959-6130

Cryptocurrency and Money Laundering

Ruiqi Wang

Abstract:

Cryptocurrency, a form of virtual currency, is increasingly pervasive in the modern society. People can use Bitcoin, Ether or Dogecoin to buy a range of products and services with ease and convenience. Yet, beneath the popularity of cryptocurrency is an emerging socio-legal concern: money laundering. Using the information collected from web sources, this brief paper taps into how cryptocurrency money laundering works and what measures can be undertaken to curtail digital crime. In view of the extant information, the paper found that a mixer is required as a 'middle man' to convert identifiable crypto-tokens into unidentifiable clean ones thereby delivering them to new wallet(s). In this manner, the origins of these tokens can be obscured, and the new tokens can be accessed and used legally. Many platforms and channels can serve as the mixer to proceed with illegal activities, including casinos, dark web marketplaces, and p2p networks. In considering the ways to tackle such digital crime in jurisdictions with limited oversight, the paper proposes to adopt measures in the Anti-Money Laundering initiatives already implemented in Hong Kong, the United States, and Singapore – especially, the need to strengthen recordkeeping to enhance the traceability and trackability of cryptocurrencies. Meanwhile, laws and rules associated with digital crime shall also be reshaped for risk mitigation.

Keywords: cryptocurrency; money laundering; digital crime; crypto-mixer; regulation

Cryptocurrency: A Driver of Money Laundering

Cryptocurrency refers to a form of digital or virtual currency that can be utilized as notes and coins for trade activities, under the protection of cryptography (Kent & Tyler, 2020). Today, various types of cryptocurrencies are active in the market, including Bitcoin, Ether, and Dogecoin. They can be used to acquire goods and services ranging from foods to real-estate investments, as long as vendor are comfortable with virtual money. Yet, with the growing popularity of cryptocurrency, some legal issues correspondingly arise. One notable concern refers to the use of cryptocurrency as a source of money laundering. This essay sets out to unpack how cryptocurrency leads to prolific money laundering and proposes measures to tackle online crime.

The underlying purpose of money laundering is whitewashing the fund collected from illicit channels. A key laundering practice is obscuring the origins of funds; in this manner, they can be legally accessed and used with minimal liabilities. According to a recent money laundering report, the advent of cryptocurrency proceeded to an innovative, tech-powered service where perpetrators take advantage of technological tools to convert the illegal funds into cash. Only through a few steps, they can conceal where the money originally comes from. From 2019 to 2023, the total amount of cryptocurrency laundered exceeded $93 billion, and $31.5bn alone in 2022 (Chain Analysis, 2024). This suggests that there had been a vast underground economy overlooked, unattended, or unaddressed by financial regulations.

The service used to proceed with laundering process is called 'mixer.' As shown in Figure 1, a crypto-mixer is designed to collect a crypto-token from an identifiable source or 'wallet', convert the token into a 'clean' one, and deliver to a different wallet. The mixer charges a fee usually between 1% and 10% for the amount laundered and creates accounts for collection and transfer merely takes a few seconds (United Nations, n.d.). The mixing or blending services beneath such a new form of digital crime are comprehensive. Convenience, unidentifiability, and rapidity allow the digital world to become a prime manufactory for laundering schemes to go prolific.

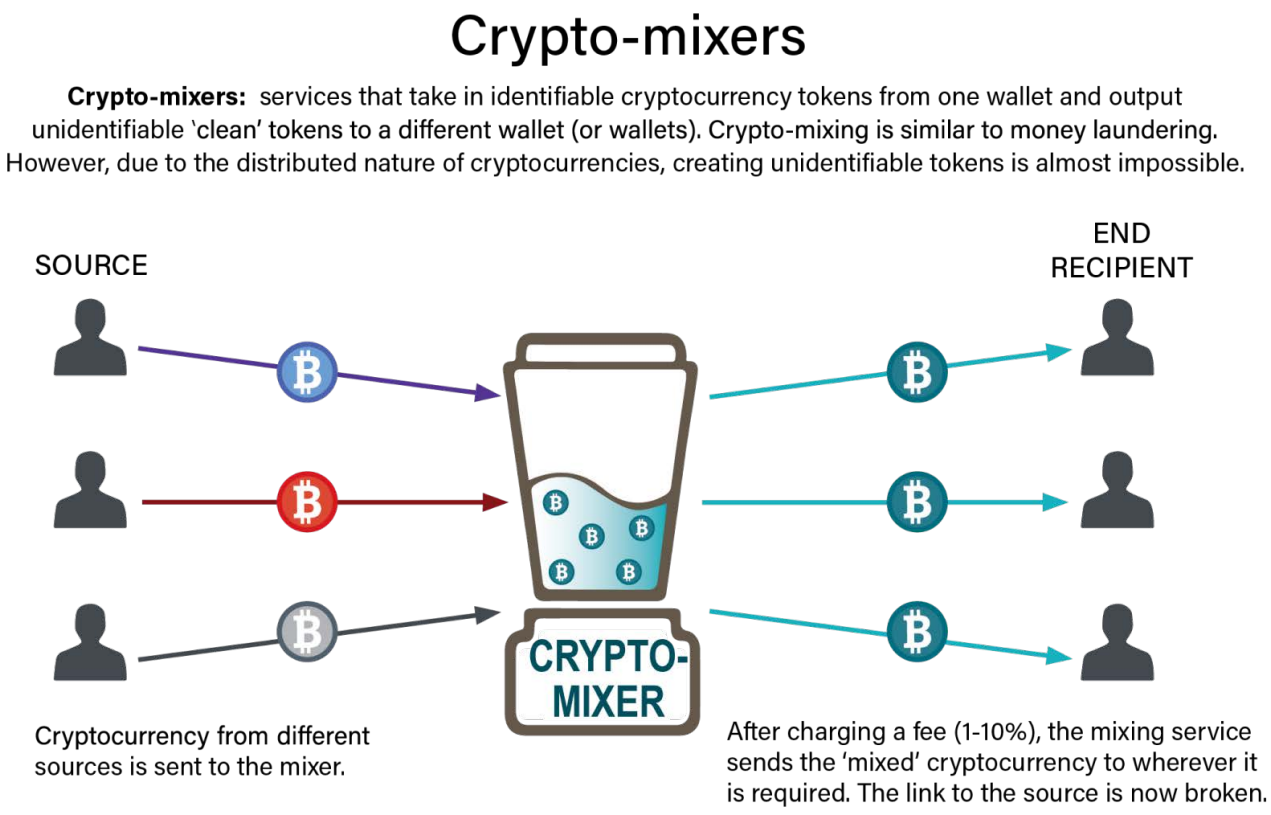

Figure 1: The middle-man role of crypto-mixer as a service installed to whitewash identifiable tokens into unidentifiable, clean ones to output wallets

Given such a vast underground economy, it is not surprising to see crypto-laundering pervasive around the globe. Recently, police in Mainland China closed a largescale laundering scheme where US$296 million was sent to South Korea. Six main suspects were arrested, for a range of accusations – one of which referred to the use of China bank accounts to collect illicit funds (Le, 2024). The funds were later used to acquire cryptocurrency at over-the-counter exchanges. The crypto was directed to ecommerce platforms and other international trade groups, finally whitewashed in South Korea. Conveyed from the case is an invaluable implication that, despite Beijing's harsh ban on commercial cryptocurrency for improving capital stability and reducing financial fraud, people are still able to find ways to proceed with underground activities.

A well-structured, tech-driven system is in presence to support transnational money laundering. United Nations (2024) notes that casinos have been playing a crucial role in catalyzing the growth and expansion of underground banking and money laundering, in particular across areas where gambling is legal. These casinos can be viewed as the 'terminals' for fast "anonymized transactions, commingling of funds, and new business opportunities for organized crime", especially online ones (United Nations, 2024). In this sense, transnational organized crime cannot be easily tackled, given the involvement of high-profile businesses and difficulty of terminating rapid online transactions. A table is constructed below (Table 1) to inform multiple channels and platforms can be utilized to conduct cryptocurrency money laundering at a transnational scale.

Table 1: Common platforms and channels used for processing money laundering

Platforms/Channels	Description
Cryptocurrency Exchanges	The point at which the trade of cryptocurrencies takes place between parties, often without oversight. For instance, OTC trading is completely free from any surveillance, which can result in money laundering activities.
Privacy Coins	Some crypto-coins are designed with strong privacy features, leading to the difficulty of tracing transactions.
Dark Web Market	Black markets concealed beneath dark web usually take cryptocurrencies as payment. The platform becomes a prime site for laundering illegal funds.
NFT marketplaces	Since non-fungible-tokens can be acquired and disposed in a way that obscures the origin of fund, perpetrators tend to use NFT as a channel to 'clean' their money.
Peer-to-Peer Network	P2P network is similarly to OTC trade, where cryptocurrencies are traded in the absence of supervision. This allows people to clean their funds across jurisdictions with weak regulations.

Conveyed from Table 1 is a notable issue: rampant crypto money laundering entails underdeveloped regulatory infrastructures that are yet to adapt to tech-induced crime. In retrospect, this 'inadaptation' appears to be understandable, given that some tech crime cannot be foreseen in prior. For instance, data security laws would not be advanced to protect and support users' digital privacy, if it were not for the lawsuits against Facebook over trading user data for interests without consent (Confessor, 2018). Also, policies and rules in relation to P2P lending would not be enhanced, if it were not for Ezubao's $7.6 billion Ponzi scheme (Tan, 2017). Thus, in several instances, regulatory improvement is not proactive, but responsive. Against emerging illegal activities, regulators and policymakers can reshape and refine current frameworks to curtail online crime and stabilize financial markets. In essence, a structured regulatory system has to rely on lessons learned from previous and current cases.

This suggests that laws and rules against crypto money laundering have been in development to tackle transnational organized crime. For instance, in Hong Kong, Anti-money Laundering (AML) legislation is being updated consistently, in response to different forms of risks associated with cryptocurrencies and flat currencies. Similarly, in the United States, AML laws and penalties are introduced and imposed on financial institutions that are tasked to "help detect and prevent financial crimes including money laundering and terrorist financing", such as recordkeeping of cash purchases, documenting any cash transactions over $10,000, assessing customer risks, and reporting suspicious activities (Lemire, 2022). As with Southeast Asia, the Monetary Authority of Singapore recently announces to tighten its AML regime, with a specific focus on user protection and stability-related protection, which affects token service providers or crypto players – for instance, unlicensed providers are obliged to notify MAS and submit a license application, or the services would be revoked (Loh, 2024). With the countermeasures taken in various parts of the world, tackling cryptocurrency money laundering shall be a global effort in need of collaboration and cooperation among jurisdictions and governments. There should be international organizations dedicated to deal with the transnational organized crimes. In addition to the UN, International Monetary Funds and World Banks may participate in the AML campaigns. With the presence and participation of these financial institutions, the overall financial stability in the global capital market can be strengthened.

In conclusion, this paper offers a brief look into how cryptocurrency aids money laundering in a tech-driven world today. The discussion above covers the mechanism of crypto laundering, with a highlight on mixers as intermediaries between the funds collected from unlawful channels and the destinations the whitewashed funds are delivered to. Due to convenience, rapidity, and unidentifiability in the virtual world, money laundering became rampant in the virtual world. International financial institutions are advised to attend these issues, in addition to the regulatory efforts by local governments. All stakeholders are expected to be on the same front to curtail online crimes.

References

Chain Analysis. (2024). *Money laundering activity spread across more service deposit addresses in 2023, plus new tactics from Lazarus Group*. https://www.chainalysis.com/blog/2024-crypto-money-laundering/

Confessore, N. (2018, Apr. 4). Cambridge Analytica and Facebook: The scandal and the fallout so far. *The New York Times*. https://www.nytimes.com/2018/04/04/us/poli-

tics/cambridge-analytica-scandal-fallout.html
Kent, P. & Bain, T. (2020). *Cryptocurrency mining*. John Wiley & Sons, Hoboken, N. J.
Le, K. (2024, May 13). Six arrested in cryptocurrency money-laundering scheme in northeast China amid focus on crypto-related capital flows. *South China Morning Post*. https://www.scmp.com/tech/blockchain/article/3262521/six-arrested-cryptocurrency-money-laundering-scheme-northeast-china-amid-focus-crypto-related
Lemire, K. A. (2022, Sept. 26). Cryptocurrency and anti-money laundering enforcement. *Reuters*. https://www.reuters.com/legal/transactional/cryptocurrency-anti-money-laundering-enforcement-2022-09-26/
Loh, D. (2024, Apr. 2). Singapore tightens anti-money laundering rules for crypto players. *Nikkei Asia*. https://asia.nikkei.com/Spotlight/Cryptocurrencies/Singapore-tightens-anti-money-laundering-rules-for-crypto-players
Tan, H. (2017, Sept. 12). Two Chinese executives get life in prison for $7.6 billion Ponzi scheme. *CNBC*. https://www.cnbc.com/2017/09/12/ezubao-two-in-china-get-life-in-prison-for-7-point-6-billion-ponzi-scheme.html
United Nations. (n.d.). *Money laundering through cryptocurrencies*. https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html
United Nations. (2024, Jan. 15). *Casinos and cryptocurrency: Major drivers of money laundering, underground banking, and cyberfraud in East and Southeast Asia*. https://www.unodc.org/roseap/en/2024/casinos-casinos-cryptocurrency-underground-banking/story.html