



2. Money Laundering Through Cryptocurrencies

Dr. L. C. Kurpatwar

*HOD, Dept. of Commerce,
Pandit Jawaharlal Nehru Mahavidyalaya,
Shivaji Nagar Chh.Sambhajinagar,
Maharashtra.*

ABSTRACT

The article's goal is to investigate the role cryptocurrencies play in the money laundering process. The article's focus is on examining the potential applications of cryptocurrencies for money laundering, as well as their limitations. issue's context. Although cryptocurrencies are widely used for a variety of purchases and transactions worldwide, the authors of the article have stressed that there is no agreement on what constitutes a cryptocurrency and its legal standing. This study aims to show that economic fraud and organized crime rely on cryptocurrency in addition to cash or other traditional currencies.

We will examine the money laundering procedure, the incorporation of cryptocurrencies into this procedure, and the responses of government and law enforcement organizations to this novel form of payment. By enabling peer-to-peer financial transactions, cryptocurrencies gradually eliminate the need for middlemen. Cryptocurrencies have been popular among the darknet and other organized crime groups because of the transparency that blockchain technology offers. With the invention of Bitcoin in 2009, cryptocurrencies have emerged as a new kind of money. The central banking system's government-backed fiat currency was supposed to face serious competition from this kind of entirely digital money. By proposing new laws to forbid the use of cryptocurrencies in money laundering, the paper adds to the ongoing conversations and arguments surrounding them. This is a study paper that discusses cryptocurrency and how they help with money laundering. We will talk about in this essay. The use of cryptocurrencies for money laundering.

KEYWORDS

Money Laundering, Cryptocurrencies, Purchasing, Transactions, Government Agencies, Blockchain, Criminals, Digital Currency, Bitcoin, Financing

1. Introduction:

A decentralized system employing cryptography to verify transactions and keep records, as opposed to a centralized authority, is what is known as cryptocurrency.

Since it is not issued by a centralized body, it is theoretically impervious to manipulation or intervention by the government. The blockchain analytics company Chainalysis claims that in 2019, criminals used exchanges to launder \$2.8 billion in Bitcoin.

The risk of money laundering and criminal activities is higher with cryptocurrencies. Compared to conventional payment methods, they offer more privacy because a transaction involving public keys cannot be traced back to a specific person. The fundamental placement-layering-integration method is followed for money laundering using cryptocurrencies, although there are several unique features:

- Since cryptocurrencies are anonymous when they are created, the placement step of the money laundering process is frequently skipped.
- Making an account (or "address") is completely free and takes only a few seconds. Each account can only be used twice: once to receive money and once to send it somewhere else.
- With a computer script, a large-scale money laundering plan involving thousands of payments can be easily created and carried out at a cheap cost.
- It is rather simple to rationalize unexpected money through cryptocurrency because to the fast rise in exchange rates, with certain cryptocurrencies experiencing growth of 10,000%.

Money Laundering Via Crypto

The financial industry is very concerned about cryptocurrencies due to their growing use and the fact that they are either less regulated or unregulated in many jurisdictions, even though they may not currently compete with cash in terms of volume of money laundered. This is also the case for the G20 Finance Ministers' and Central Bank Governors' 2019 summit in Japan. A note from the meeting said, "Although crypto-assets do not currently pose a threat to global financial stability, we remain vigilant to risks, including those related to consumer and investor protection, anti-money laundering, and countering the financing of terrorism."

Crypto advisers frequently assert that using cryptocurrencies for money laundering is an inefficient approach when compared to traditional methods because it is extremely dangerous and complicated. Additionally, they contend that when compared to fiat currencies, transactions involving digital currencies are more accountable and transparent. Another viewpoint is that there is relatively little money laundering utilizing cryptocurrencies, and that the media in general prefers to focus on criminal activity involving digital currencies over advancements in technology and innovation. Without a doubt, cryptocurrencies are being used to help in money laundering, even if it's only on a limited scale. [1]

Cryptocurrency Money Laundering Work:

To hide their origins, criminals use a variety of services and procedures that route money through multiple addresses or companies. After then, the assets are transferred from what appears to be a reliable source to a destination location or an exchange for liquidation. It is exceedingly difficult to link money that has been laundered to illegal activity thanks to this procedure.

The top 5 techniques used by thieves to launder money on the blockchain are listed below.

Services that function inside one or more exchanges fall under the large category of nested services. In order to take advantage of trading opportunities, these services use addresses hosted by the exchanges to access the exchanges' liquidity. Certain exchanges have lax compliance requirements for nested services, which makes it possible for dishonest people to use them as a means of money laundering.

These transactions involving nested services seem on the blockchain ledger to have been carried out by their host counterparties, or the exchanges, as opposed to the hosted nested services or the addresses of the individuals involved.

Over-the-Counter (OTC) brokers are the most prevalent and well-known kind of nested services. Large-scale cryptocurrency trading is made simple, safe, and anonymous for traders via OTC brokers. OTC brokers act as middlemen between two parties to enable direct cryptocurrency trades without the need for an exchange. These trades can be done between fiat currencies, like euros, and cryptocurrencies, like Bitcoin, or between cryptocurrencies and other cryptocurrencies, such as Ethereum and Bitcoin. In return for a commission, the OTC brokers locate counterparties for a transaction; they do not participate in the talks. The parties give the broker custody of the assets once the arrangements have been agreed upon.

Cryptocurrency money launderers frequently use gambling platforms. Money is deposited onto the network via a mix of recognizable and anonymous accounts. They are either wagered or cashed out, frequently in concert with affiliates. After the funds in the gambling account are disbursed, it may be granted legal standing. The Financial Action Task Force's (FATF) September 2020 report, titled "Virtual Assets Red Flag of Money Laundering and Terrorist Financing," includes information on gambling services.

In order to increase anonymity, mixers are services that combine digital assets from many addresses before releasing them sporadically to new destination addresses or wallets. They are frequently employed to hide the trail of money before it is moved to reputable companies or significant exchanges.

Fiat exchanges can be mainstream, peer-to-peer (P2P), or non-compliant (exchanges that do not follow or are not subject to rules). **They convert cryptocurrencies into cash.** Conventional financial investigative techniques need to be used after monetary exchanges have occurred.

Services in countries designated as having strategic shortcomings in their AML or Combating the Financing of Terrorism (CFT) regimes are those with headquarters in high-risk jurisdictions.

Cryptocurrency and money Laundering:

Criminals use digital currency exchanges, which take fiat money from conventional bank accounts, to open online accounts. After that, they begin the "cleansing" process (mixing and layering), which involves transferring funds into the cryptocurrency system through the use

of tumblers, mixers, and chain hopping, also known as cross-currency mining. A nearly impossible-to-track money trail is created when money is transferred between cryptocurrencies and between digital currency exchanges; the less regulated the better.

The "Cryptocurrency Anti-Money Laundering Report" claims that thieves and gamblers also utilize cryptocurrency laundering as a means of financial gain.

The establishment of the Dark Web or Dark Market led to the use of hacking to take advantage of users.

As the largest cryptocurrency globally, bitcoin has a market valuation of \$350 billion. One of the unique characteristics of bitcoin is that all transactions are kept in a public ledger that is concurrently updated on hundreds of computers. Cryptocurrency advocates claim that the latter are vulnerable to manipulation or hacking.

Legal tender does not exist for cryptocurrency. As a result, money laundering occurs because it is not approved and anyone can subscribe.

It is simple to transact between nations and has the potential to facilitate money laundering under the cover of commerce because it lacks regulatory power. [2]

Cryptocurrency Money Laundering Risks

Due to their increased degree of anonymity, cryptocurrencies are more vulnerable to money laundering and other illegal activity threats. It is more difficult to track the source and destination of transactions when one's identity is unknown, particularly on platforms with lax AML and KYC procedures.

It's possible for a single cryptocurrency wallet to be connected to numerous credit cards and banks, which suggests that multiple people are using the wallet to transfer money around.

Operating under many jurisdictions is challenging for law enforcement in the absence of a central administrator. Therefore, in the event that poor or nonexistent AML controls are implemented, fraudulent trading operations may remain undetected.

Money Laundering in cryptocurrency

Cryptocurrencies are a great option for money laundering because of their intrinsic anonymity, ease of cross-border transactions, and decentralized peer-to-peer payments. Imagine being able to purchase any quantity of bitcoin (or any other cryptocurrency) through an exchange, casino, or online gaming in one nation, then cash it in anywhere in the globe.

Anti-money laundering laws and regulations have been adopted in many countries; however, it is still difficult to execute and ensure actual compliance. Blockchain provides solutions for anti-money laundering compliance, which is essential for stopping money laundering. The following are some positive behaviors that can make life harder for wrongdoers:

The ledgers on the blockchain cannot be altered. This indicates that all transactions are permanently logged on it. This creates a wonderful chance for oversight. Scalable technology solutions with AI support can be an excellent automated tool.

Respecting KYC regulations can significantly reduce the likelihood of money laundering. Each transaction can have a blockchain-based network linked to it that records authenticated identity. These ledgers can be managed by exchanges, and this activity can be facilitated by tech companies.

Smart contracts built on the blockchain can be used to guarantee AML compliance. To ensure the success of the transactions, the smart contracts can be built to incorporate different parameters, and any abnormality can be flagged by ML-based algorithms.

Providers of blockchain analytics can assist with frequent updates on compliance and anomalies that raise red flags. This guarantees an appropriate system and audit trail for transactions and upholds AML compliance. [3]

Review of Literature:

As of right now, Bitcoin is the most widely utilized cryptocurrency with bidirectional flow. A decentralized P2P (person to person) payment network, Bitcoin operates without the need for intermediaries or central authorities. As far as users are concerned, Bitcoin is similar to cash—but only on the Internet (Bitcoin information website). There is a limit on the total amount of Bitcoin in the world, and it cannot exceed 21 million. The person known only as Satoshi Nakamoto is credited with creating Bitcoin. On September 3, 2009, he published an article titled "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2009) on the Internet, outlining the key ideas behind the new cryptocurrency. One of the key differences between Bitcoin and other electronic money systems and cashless settlements is that Bitcoin does not have issuer debt. [4]

For the most part, cryptocurrencies are viewed as competitors to the traditional money that is supported by financial institutions. However, because no federal body supports cryptocurrencies, their financial foundation is unknown and subject to large fluctuations. But whether blockchain is a true asset store (like gold), a monetary unit (like the US dollar), or a hybrid of the two is still up for debate within the scientific community and the financial markets (Hayes, 2017). [5]

A new class of "digital" cash known as cryptocurrencies was introduced in 2009 when Satoshi Nakamoto created Bitcoin. To put it more simply, a cryptocurrency is a set of code that is recorded in an accessible shared database and permits peer-to-peer exchanges without the need for a middleman. The "blockchain" is a vast network of computers that can validate each database money transfer. This network is where the software used for cryptocurrencies is encrypted and verified. Even if the blockchain is legitimate, it is quite challenging to pinpoint a company or an individual for a particular transaction on the blockchain. Certain cryptocurrency exchanges, like those listed by Dash, Litecoin, and Bitcoin, are hard to use but traceable, but other exchanges, like Monero and Zcash, conceal every transaction, making it hard to identify and identify financial transactions (Deepika, 2017). [6]

Effective measures are urgently needed to combat and mitigate the impacts of the serious problem of money laundering alongside terrorist financing within the European Union. The financial and economic sector's stability, integrity, reputation, and performance are all at risk (Shaikh et al. 2021). The amount of research, literature, and specialist studies on financial and economic crimes is increasing, but more work in the area is required. In particular, further work must be done to close the gaps by using empirical analysis to determine the extent of the unorganized sector, its causes, their methods, and correlations, as well as the impact on financial and economic crimes. [7]

Objectives:

- Cryptocurrencies offer a level of anonymity that traditional financial systems lack, enabling money launderers to obscure transaction origins effectively.
- To Study of Money Laundering Through Cryptocurrencies
- To Process of Cryptocurrency Money Laundering Works

Research Methodology:

Journal papers and commentary will be used as secondary legal sources of data in the research. While highlighting matters of concern, the commentaries will offer some explanations that the commenters and the interpretation of the law are expected to provide (Benson 110). A descriptive study of the statute will be produced by utilizing data from both primary and secondary sources. Secondary sources will be used in this study because, according to the Association of Certified Fraud Examiners, they offer criticism on the efficacy of the law rather than restricting its description. Furthermore, secondary sources will include non-legal sources in addition to journal papers published in the legal field.

Result and Discussion:

Crypto Used for Money Laundering:

It is true that money laundering has been accomplished with cryptocurrency use. The semi-anonymous feature of many cryptocurrencies allows criminals to hide the source of unlawful cash, much like traditional financial systems.

It's important to note, though, that governmental actions, increased monitoring, and developing blockchain analytics are making it harder for bad actors to exploit cryptocurrencies for money laundering.

In 2021, cybercriminals used DeFi protocols to launder their cryptocurrency funds more than they did in 2020, according to a Chainalysis analysis. According to a new Chainalysis analysis, in 2021, cryptocurrency was used to launder \$8.6 billion in value. Although it is up 25% from 2020, it is still far behind the peak watermark reached in 2019.

In that year, cryptocurrencies were used to launder \$10.9 billion in value. According to Chainalysis, \$33.4 billion in cryptocurrency has been laundered since 2017.

Money Laundering Through Cryptocurrencies

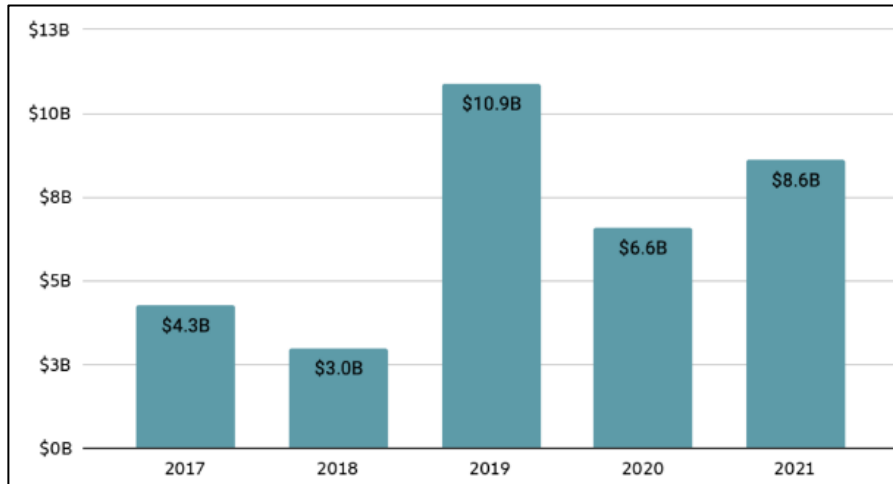


Figure 1: Total Cryptocurrency Value Laundered by Year, 2017 – 2021 [8]

According to Chainalysis, the estimated \$2 trillion in fiat that is laundered annually from offline crimes like drug trafficking dwarfs the \$33.4 billion in cryptocurrency that has been laundered since 2017. However, because offline crimes sometimes employ untraceable cash, it is more challenging to get an accurate estimate of the quantity of money laundered than with cryptocurrency.

The 2023 analysis from Chainalysis states that criminal activity utilizing cryptocurrency peaked in 2022 at a total of \$20.6 billion. Notably, 43% of the year's illicit transaction volume was associated with firms under sanctions, which corresponded with the imposition of some of OFAC's most ambitious and difficult-to-enforce crypto limitations.

Table 1: Reasons for Sanction

Name	Reason for sanction
Lazarus Group	Hacking and crypto theft on behalf of North Korean government
Ahmad Khatibi Aghada	Ransomware
Amir Hossein Nikaeen Ravari	Ransomware
Alex Adrianus Martinus Peijnenburg	Drug trafficking
Matthew Simon Grimm	Drug trafficking
Hydra Marketplace	Darknet market and money laundering
Garantex	Money laundering
Blender.io	Money laundering
Tornado Cash	Money laundering
Task Force Rusich	Russian paramilitary group in Ukraine

Although they can be used as a conduit for money laundering, cryptocurrencies only make up a small percentage of total money laundering operations worldwide. There are ongoing initiatives to reduce the improper use of these virtual currencies.

Exchanges Receiving Illicit Bitcoin in 2019:

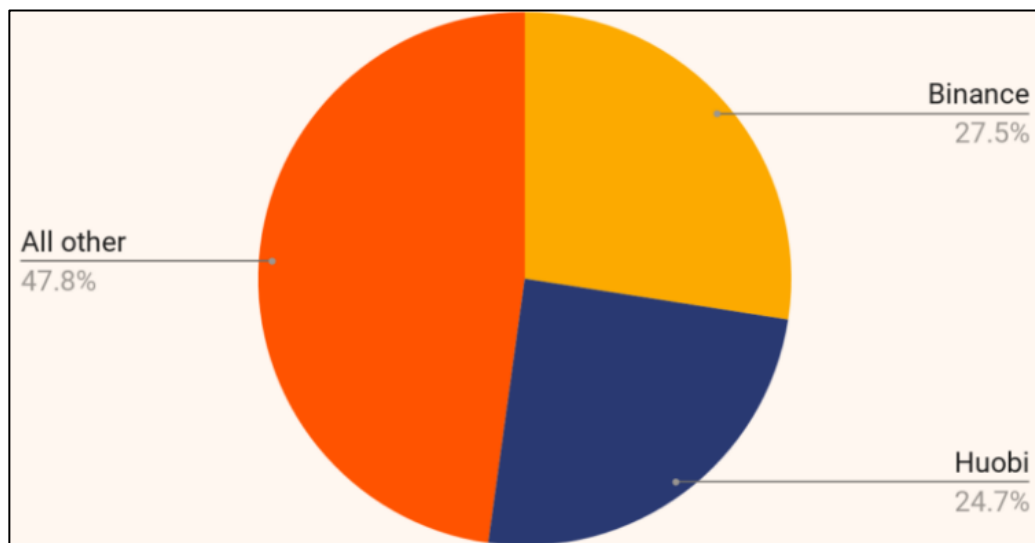


Figure 2: Exchanges Receiving Illicit Bitcoin in 2019

By a wide margin, Binance and Huobi are the top two cryptocurrency exchanges for receiving illegal Bitcoin. Considering that Huobi and Binance are two of the biggest exchanges in operation and are governed by KYC laws, that could surprise some.

In total, in 2019 little over 300,000 distinct Binance and Huobi accounts got Bitcoin from illicit sources. The total value of all the Bitcoin that those accounts have received in 2019 is broken down into buckets below, with illicit Bitcoin highlighted. Please take note that this chart only takes into account \$1.1 billion of the \$1.4 billion in illicit Bitcoin that Binance and Huobi have received. This is because of the way we link illicit funds to specific addresses.

There is no financial institution affiliated with the ruling party to contact when using digital currencies as a shell corporation. Consequently, dishonest businesses and illicit groups will convert their earnings into cryptocurrency holdings, which they will then transfer throughout the globe to evade tax authorities. Because it gives illegal businesses better access to and control over all of the money they make, this increased protection benefits the money laundering system. It is anticipated that the use of cryptocurrencies in the cycle of money laundering would have significant effects on global economies. Governments have historically faced significant challenges as a result of money trafficking. Money laundering has gotten beyond organized financial constraints since the creation of the central banking structure by positioning, stratifying, and convergent strategies. Because of its secrecy, cryptocurrency is strongly associated with money laundering. Criminal organizations can more successfully channel money to avoid being prosecuted by the government by using cryptocurrencies in the money laundering process. [9]

Mixing and Tumbling:

New technologies are also being utilized to launder cryptocurrency and make filthy money appear clean, even if many of the examples discussed thus far have shown updated versions of conventional money laundering strategies.

A technique called "mixing," which is sometimes known as "tumbling," is among the most cunning. The idea is comparable to a mutual fund, where different people can pool their money together for the group's ultimate benefit. But rather of investing, the pooled funds are transferred between exchanges, which makes it very challenging to track down individual transactions (Cryptocurrency Anti-Money Laundering Report, 2018). Below is a screenshot of the CipherTrace report that illustrates the mixing procedure:

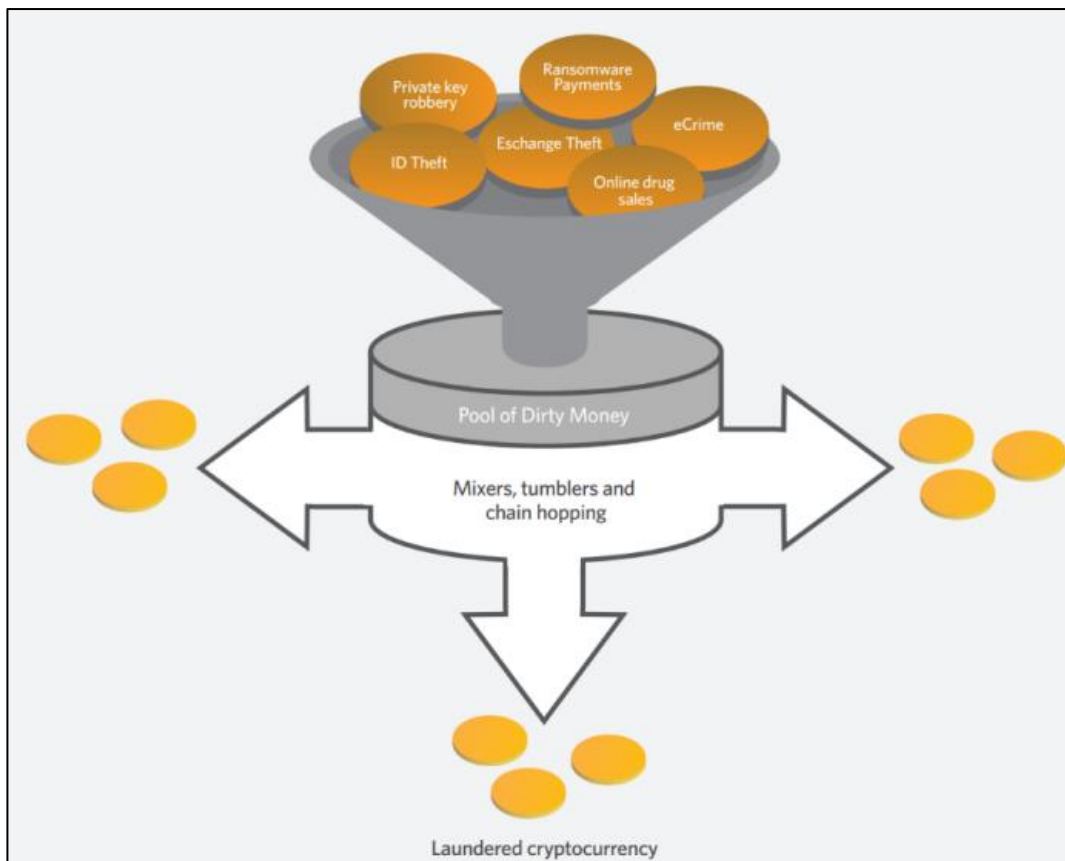


Figure 3: Laundered Cryptocurrency

Mixer:

In addition to mixing/blending methods pertaining to "normal" cryptocurrencies, there are specialized services for this purpose accessible on the market.

In order to hide their origin and render cryptocurrency funds untraceable, a number of systems "mix" or "blend" potentially identifiable funds. First, cryptocurrency coins (the funds) are sent to one address (the account) from many sources.

The money is divided into multiple parts and distributed to various addresses after it has been combined or blended in that one address. Prior to the money arriving at its intended location, this procedure could be carried out multiple times.

It is therefore nearly impossible to trace the monies back to their original source.

Member states must enact appropriate cryptocurrency market regulation and oversight in order to mitigate the associated risks.

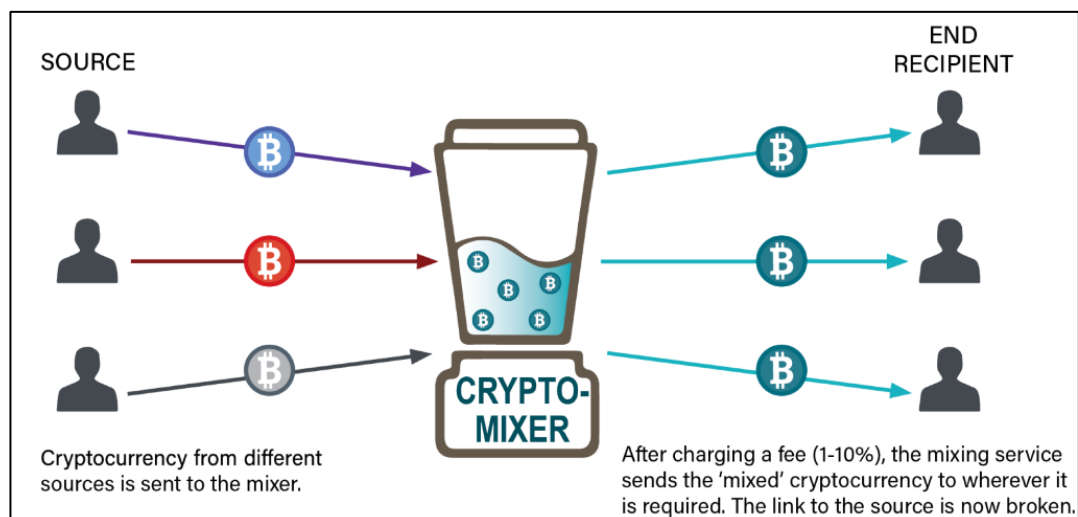


Figure 4: Crypto-Mixer

Cryptocurrency Money Laundering Process Works:

The classic money laundering method consists of three separate stages: integration, layering, and placement. During the placement phase, when cash is typically used for money laundering, the illicitly obtained dirty money is initially injected into the banking system.

Large cash deposits can raise suspicions, thus even though there are many ways to avoid getting detected, this is the stage where the money launderer is "most vulnerable to being caught" (Money Laundering: A Three Stage Process, n.d.).

The money is transferred across accounts, goods, financial organizations, and even to other nations and currencies throughout the layering phase, making it challenging to track the money back to its original source. Eventually, the cleaned and "laundered" money is given back to the criminal during the integration stage, seeming as though it was obtained rightfully this time. The chart below, called KYC Map, also shows the multi-stage process:

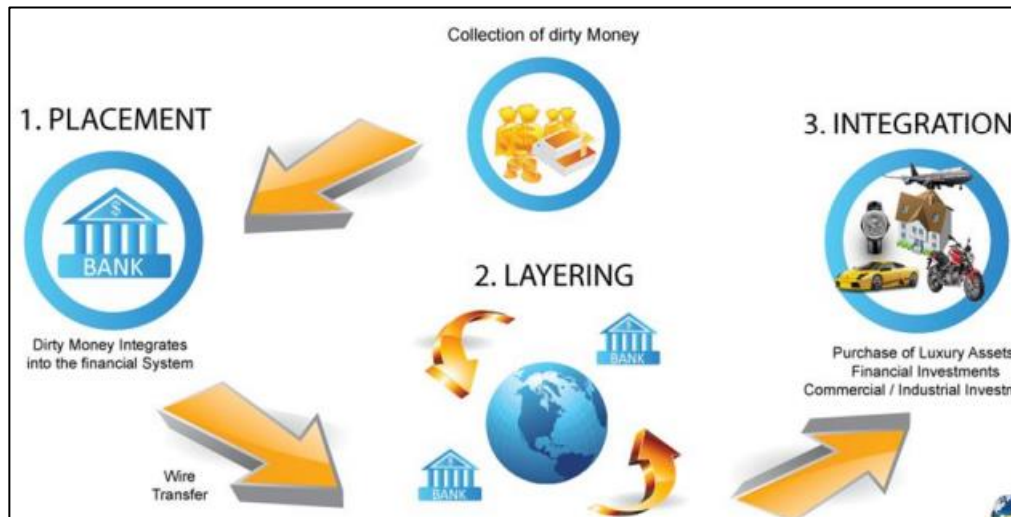


Figure 5: A Typical Money Laundering Scheme [10]

Conclusion:

There's little doubt that regulations pertaining to cryptocurrencies will grow in the future. Similarly, present trends indicate that several government bodies will likely soon enhance their regulation of AML.

Regulators are still creating oversight over this expanding industry even though there are many safe harbors and regulatory gray areas.

References:

1. Graeber, D. (2015). *Debt: The first 5000 Years*. Ad. Marginem Press. Moscow. (in Russian)
2. Pelo, A. (2015). Virtualization of the global banking system in the context of globalization. *Visnyk ONU im. I. I. Mechnikova*.
3. Albrecht, C., Duffin, K.M., Hawkins, S. and Morales Rocha, V.M. (2019), "The use of cryptocurrencies in the money laundering process", *Journal of Money Laundering Control*, Vol. 22 No. 2, pp. 210-216. <https://doi.org/10.1108/JMLC-12-2017-0074>.
4. Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from: <https://bitcoin.org/bitcoin.pdf> (accessed 30 October 2018)
5. Hayes, A.S. (2017), "Cryptocurrency value formation: an empirical study leading to a cost of production model for valuing bitcoin."
6. Deepika, P. (2017), "Cryptocurrency: trends, perspectives, and challenges", *International Journal of Trends in Research and Development*, [online], Available at: [Accessed 23 May 2020].
7. Shaikh, Abdul Khalique, Malik Al-Shamli, and Amril Nazir. 2021. Designing a relational model to identify relationships between suspicious customers in anti-money laundering (AML) using social network analysis (SNA). *Journal of Big Data* 8: 1–20.

8. Amrani, Hanafi and Mahrus Ali. "A New Criminal Jurisdiction to Combat Cross-border Money Laundering." *Journal of Money Laundering Control*, 2021, Web.
9. Association of Certified Fraud Examiners. *Fraud Examiners Manual*. ACFE, 2021.
10. Crosman, P. (2018, September 8). Retrieved from American Banker: Crosman, P. (2018, July 03). Crypto money laundering up threefold in 2018: Report. Retrieved from <https://www.americanbanker.com/news/crypto-money-laundering-rose-3x-in-first-half2018-report>.