International Journal for Multidisciplinary Research (IJFMR)

E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Money Laundering Using Cryptocurrency

Mahendran Varma[1], Dr. Batani Raghavendra Rao[2]

[1]Student, MBA (International Finance and Accounting) in JAIN (Deemed-to-be University) CMS Business School
[2]Professor at JAIN (Deemed-to-be University) CMS Business School

Abstract

The main purpose of this study is to provide a comprehensive assessment of the importance of cryptocurrencies in terms of money laundering risk and to provide detailed information on money laundering techniques and structures. An analysis of how cryptocurrencies impact local and international money laundering is also being explored to clarify the facts. The article attempts to provide a better understanding of this emerging problem by providing information on the use of digital currency to change the money laundering landscape. To clarify the review, the review is divided into two main parts: The first part will focus on the theoretical framework of the money laundering process, the process complexity of cryptocurrencies and the ecosystems surrounding them. The second part will examine whether virtual currencies are suitable for money laundering, the various features that make virtual currencies ideal for such activities, and the creation of new emerging technologies will also be discussed. This document is designed to provide policymakers, regulators, and law enforcement with useful information and strategic solutions to address the challenges of cryptocurrency money laundering through many of these methods.

Keywords: Cryptocurrency, Money Laundering, Anti-Money Laundering Measures, Blockchain Technology, KYC (Know your Customer).

1. Introduction

It was in April 2018, when the Reserve Bank of India (RBI) prohibited all banks and regulated entities from dealing with or providing services to any individual or business dealing with virtual currencies, citing possible risks such as money laundering and terrorist financing. However, in March 2020, the Supreme Court of India overturned this ban, allowing individuals and businesses to trade in cryptocurrencies. It is important to note that the legal status of cryptocurrencies in India is still somewhat unclear, as the government has yet to issue specific regulations on the same. This paper aims to evaluate the significance of virtual currencies concerning the risk of money laundering within the market. Additionally, it identifies common money laundering techniques and identifiable patterns of misuse. The analysis commences by considering the theoretical basis of money laundering tactics. The paper also evaluates the extent to which virtual currencies are suitable for laundering money, highlighting the characteristics that facilitate such activities. The document also examines unique money laundering methods arising from the usage of virtual currencies.

In India, the Prevention of Money Laundering Act (PMLA) was enacted in the year 2002 and was amended in 2005 to include provisions for offences related to money laundering. In 2013, the Reserve Bank of India (RBI) issued warnings about the use of cryptocurrencies for illegal activities, including money laundering. In 2018, the RBI imposed a ban on banks dealing with entities involving virtual currencies. However, the ban was lifted by the Supreme Court of India in 2020, which provided opportunities for cryptocurrency companies to operate with greater ease. Nonetheless, the RBI issued a statement advising banks to remain cautious when dealing with cryptocurrency-based businesses due to concerns about money laundering and other illegal activities.

Approach: The study carefully collected information from secondary sources and on-the-ground events to explore the complex world of money laundering afforded by cryptocurrencies. The study intended to discover widespread patterns and developing trends in the unlawful use of cryptocurrencies for money laundering by a thorough investigation of academic publications, government reports, court documents, and existing literature. Researchers aimed to comprehend the particular strategies used by individuals and criminal groups to use cryptocurrency for money laundering by looking at real-world instances from court cases. The research yielded important insights into the favoured cryptocurrencies, money laundering strategies, and geographic hotspots linked to illicit operations through the use of both quantitative and qualitative analysis methodologies. Ultimately, the study's findings provide valuable insights for policymakers, regulators, and law enforcement agencies, offering recommendations to enhance regulatory frameworks, technological tools, and international cooperation in combating cryptocurrency-related money laundering

2. Review of Literature

1. The use of cryptocurrencies in the money laundering process. Journal of Money Laundering Control by Albrecht, C., Duffin, K., Hawkins, S., & Rocha, V. (2019). – This paper highlights how Cryptocurrencies, due to their anonymity and direct peer-to-peer transactions, have become a popular choice for money laundering due to their lack of intermediary financial institutions.
2. Cryptocurrency In The System Of Money Laundering. by Dyntu, V., & Dykyi, O. (2019). The paper discusses how Cryptocurrencies are a convenient tool for money laundering due to their relative anonymity and decentralization, making it difficult for law enforcement agencies to track criminal activity and identify criminal personalities.
3. A Framework to Build User Profile on Cryptocurrency Data for Detection of Money Laundering Activities by Samanta, S., Mohanta, B., Pati, S., & Jena, D. (2019). - This study proposes a framework to convert Bitcoin's transnational data into a similar bank's user database, which can help detect money laundering activities by analyzing abnormal clusters of transactions and user behaviour.
4. An Abnormal Transaction Detection Mechanism on Bitcoin by Yang, L., Dong, X., Xing, S., Zheng, J., Gu, X., & Song, X. (2019) - This paper proposes a method to detect illegal activities in Bitcoin by mining user characteristics, clustering suspicious users, and detecting abnormal transactions among them.
5. Understanding Money Trails of Suspicious Activities in a cryptocurrency-based Blockchain by Lal, B., Agarwal, R., & Shukla, S. (2021) – This paper gives a heuristics-based approach using hidden patterns in temporal transactions graphs can analyze and find suspicious activities in cryptocurrency blockchains, such as gambling, phishing, and money laundering.
6. SoK Money Laundering in Cryptocurrencies by Kartik Kolachala, Ecem Simsek, Mohammed Ababneh, Roopa Viswanathan (2021) – This paper discusses the rising trend of money laundering through cryptocurrencies and the response of regulatory authorities with stricter anti-money laundering (AML) measures.

7. On Modern Crime – Money Laundering and Cryptocurrencies by Justyna Meszka (2023) This paper explains how cryptocurrencies' anonymity and technology advancements make them attractive for money laundering, allowing for the creation of new criminal methods.
8. Virtual Money Laundering: Policy Implications of the Proliferation in the illicit use of cryptocurrency by Christian Leuprecht, Caitlyn Jenkins and Rhianna Hamilton (2022) – This paper aims to explain how cryptocurrency is leveraged for illicit purposes across the global financial system. Specifically, it establishes how cryptocurrency has been changing the nature of transnational and domestic money laundering (ML)
9. Cryptocurrency and money laundering: A literature review by Achraf Guidara (2022) – This paper focuses on empirical research in the accounting and finance fields that deal with the impact of cryptocurrencies on the phenomenon of money laundering.
10. Money Laundering Through Cryptocurrencies by Fabian Maximilian Johannes Teichmann, Marie-Christin Falker (2020) – The paper analyzes compliance risks associated with cryptocurrencies and how they can be used for money laundering, based on interviews with compliance officers and presumed criminals.

3. Regulatory Bodies

Global standards: Financial Action Task Force (FATF):

The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. FATF has developed 40 FATF Recommendations, which ensure a coordinated global response to prevent organised crime, corruption and terrorism. They help authorities go after the money of criminals dealing in illegal drugs, human trafficking and other crimes. There are more than 200 countries and jurisdictions committed to implementing the Recommendations. FATF reviews money laundering and terrorist financing techniques and continuously strengthens its standards to address new risks, such as the regulation of virtual assets, which have spread as cryptocurrencies gain popularity. FATF monitors countries to ensure they implement the FATF Standards fully and effectively through a process of Mutual Evaluation Reviews and holds countries to account that do not comply. In consultation with members of the accounting profession, FATF has issued various recommendation publications including those relating to the Risk Based Approach for Accountants.

European Union:

In June 2018, the Directive (EU) 2018/843 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for money laundering or terrorist financing (the 5th AMLD) became law. The AML Directive (AMLD) is the cornerstone of the European Union's (EU) anti-money laundering and countering the financing of terrorism (AMUCFT) policy.

Channel Islands and Isle of Man

1. Channel Islands:

Members in the Channel Islands or Isle of Man are not subject to UK legislation but must signify that they are aware of the legislation on AML passed in their respective jurisdiction, e.g. Guernsey or Jersey, as appropriate.

2. Isle of Man

The Department for Home Affairs (DHA) provides legislation and guidance on anti-money laundering requirements for the Isle of Man.

All businesses that accept cash payments of 15,000 Euros or more, or the equivalent in any currency including sterling, or are of a designated type (see below for further information), are required to comply with legislation regarding the prevention of money laundering and terrorist financing (ML/TF) further to the requirements of the Proceeds of Crime Act 2008 (POCA) and the Terrorism and Other Crime (Financial Restrictions) Act 2014. The relevant secondary legislation was last updated via the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 [SD 2019/0202], which came into operation on 1st June 2019, and by the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Code 2019 [SD 2019/0219], and Anti-Money Laundering and Countering the Financing of Terrorism (Specified Non-Profit Organisations) Code 2019 [SD 2019/0200], that both also came into operation on the same date. In December 2019 the Anti-Money Laundering and Countering the Financing of Terrorism (General and Gambling) (Amendment) Code 2019 [2019/0457] was made which amends SD 2019/0202 and SD 2019/0219.

People's Republic of China

The PRC Anti-Money Laundering Law and the PRC Counter-Terrorism Law systematically set out anti-money laundering requirements for all financial institutions established within the PRC and certain non-financial institutions that have AML obligations.

The People's Bank of China as the primary regulatory authority of AML issues, has promulgated various regulations and rules that stipulate specific AML requirements of reporting entities in conducting their business (e.g. the Measures on the Administration of the Customer Identity Verification and the Identification and Transaction Document Keeping by Financial institutions).

The China Banking & Insurance Regulatory Commission and the China Securities Regulatory Commission as the regulators of banking, insurance, and securities sectors, respectively have also published rules that impose specific AML requirements on financial institutions regulated by these organisations (e.g. the Implementation Measures of the AML Work in Securities and Future Sectors).

The PRC underwent a FATF Mutual Evaluation Review in 2019 and a follow-up report was issued in 2020 which explored progress made in strengthening money laundering and terrorist financing controls.

US requirements

The United States of America has federal anti-money laundering laws and 38 of the 50 US states have AML laws. Some of these state regimes merely establish reporting requirements, while others either mirror federal law or, in some cases, are more stringent than federal law.

During the 1990s, a series of AML laws were enacted to strengthen the AML regime. The most significant of these laws was the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 ('the Patriot Act'), which was passed into law in the immediate aftermath of the 11 September terrorist attack. The Patriot Act amended The Bank Secrecy Act (BSA) to strengthen the government’s ability to prevent, detect and prosecute international money laundering and the financing of terrorism.

Transparency International

Transparency International (TI) is a global movement working in over 100 countries to end the injustice of corruption.

TI works to expose the actors, methods and systems that the corrupt depend upon to facilitate the laundering, transfer and investment of dirty money.

4. Crypto-Based Money Laundering Methods:

MIXING

It is a technique called cryptocurrency mixer, also known as a tumbler. It is utilized to mix coins that may be identifiable or tainted with others to obscure the trail leading back to their source. By combining inputs from multiple sources for an extended and random period before dividing them up into destination addresses, it becomes difficult to track specific coins. Tumblers have arisen due to the need for anonymity when dealing with digital currencies since all transactions are publicly recorded on a ledger. Due to its secrecy objective, tumblers have been utilized to cash-wash cryptocurrency.

The Sheep Marketplace incident that occurred in December 2013 is a great illustration of how tumbling works in reality. The marketplace was created to cater mainly to illegal activities like selling drugs and weapons, along with stolen data that was ripe for exploitation. In this case, thieves stole over $8 million worth of Bitcoin, causing shockwaves across digital currency marketplaces worldwide. To protect themselves from being tracked by authorities, they used Bitcoin Fog, which had been operational between 2011 and 2021, offering obfuscation tools via shared pools whereby users’ coins were merged, making the retracing task demanding. However, even though some individuals use these services hoping not to leave any traces linking them, in the end, they can't hide behind the blockchain transparency layer technology. While mixing tools offer temporary relief through veiled pathways, ultimately, blockchain's transparent nature plays its part in revealing the truth around every corner, reminding us of the responsibilities required in developing technologies responsibly. It urges positive collaboration among regulators, developers, and law enforcement agencies to secure future records clean and avoid illicit trade, promoting ethical practices when trading crypto-assets.

FIAT-TO-CRYPTO EXCHANGE

So basically, a fiat-to-crypto exchange is like a marketplace where you can swap regular money for cryptocurrencies like Bitcoin and Ethereum. Places like Coinbase and Gemini let folks trade their dollars, euros, whatever for digital coins. It kinda bridges the gap between traditional finance and the crypto world. These exchanges make it easy for people to buy and sell all sorts of digital assets in one spot. They act as a go-between so folks can access cryptocurrencies and mess around with that newfangled financial tech. It provides both convenience and a way to dip your toes in the crypto waters, resulting in pretty neat ways to connect regular finance and the emerging crypto ecosystem. These platforms act as trusted matchmakers, enabling users to buy, sell, and trade a myriad of digital assets, offering both convenience and access to this innovative financial frontier.

The case of the Garantex cryptocurrency exchange provides a prime example of the challenges associated with regulating exchanges that facilitate transactions between cryptocurrencies and fiat currencies. The blacklisting of Garantex, a Moscow-based crypto exchange, in 2022 exposed vulnerabilities in regulating such crypto-fiat exchanges. Garantex's ability to bypass sanctions on Russian rubles, coupled with its opaque operations and acceptance of cash deposits, raised legitimate concerns about its potential role in sanctions evasion, money laundering, and possibly even aiding sanctioned entities like Hamas. While the exact extent of Garantex's illicit activities remains under ongoing investigation, this case serves as a stark reminder of the difficulties posed by the rapid evolution of the cryptocurrency market and the urgent need for robust international cooperation, stricter anti-money laundering and know-your-customer frameworks, and enhanced transparency within the cryptocurrency ecosystem to ensure its contribution to a secure and inclusive financial future, not as a haven for unlawful conduct.

PRIVACY ORIENTED COINS

Privacy coins are cryptocurrencies with privacy-enhancing features designed to boost anonymity and reduce traceability. They operate similarly to physical cash, but within a digital ecosystem, the largest of which is called Monero Monero works to avoid identification and verification, by focusing on improved anonymity and security in payments. Monero, established via a split from the cryptocurrency Bytecoin in 2014, both obscures the digital addresses of those involved in a given payment and hides the value of every crypto transaction. So, it becomes much harder to identify users.

Monero accomplishes this through two key methods. First, it employs “stealth addresses.” While every Monero wallet has a public view and public send key, these wallet addresses aren’t used to send transactions themselves. Instead, with every transaction the ledger records a one-time stealth address generated using those public view and send keys. With these one-time addresses, only the sender and recipient are aware of who owns the sending wallet. Second, Monero and most other privacy coins rely on another strategy known as a ring signature. In essence, this is transaction mixing; instead of just one account sending a transaction, a “ring” of users signs the transaction and “sends” it alongside the actual originator of the payment. Thus, it becomes extremely difficult to identify who the real sender is even if you were able to identify the owner of the one-time stealth addresses.

Due to its non-public blockchain and concealed transaction amounts, Monero has been used by some to evade law enforcement detection and avoid regulatory oversight. Many individuals and organizations appreciate Monero's privacy features. Despite its growing popularity, the regulatory environment around Monero remains uncertain. Because its privacy features make it difficult to track and identify users, lawmakers and regulators around the world may hesitate to embrace it fully. This may limit its adoption and use as a mainstream cryptocurrency. However, because of its privacy features which make transactions untraceable and anonymous, Monero has become a popular option for criminal activities such as money laundering and the purchase of illegal goods on dark web marketplaces. The Privacy coin works in the following ways:

- Stealth addresses enable the creation of a new address every time a user receives a cryptocurrency. Monero utilizes this method by generating a public address, a private view key to display incoming transactions, and a private spend key for sending funds.
- Ring signatures join together multiple users in a “ring” to hide their identities, making it more difficult to determine which user generated a given signature. This is how Monero and Bytecoin obscure transactions.
- Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) involves using cryptography to prove that a transaction is valid without revealing the details of the transaction. Zcash was the first privacy coin to apply zk-SNARKs on a large scale.

ONLINE GAMBLING

Cryptogambling combines conventional gambling with cryptocurrencies, incorporating blockchain technology into the gambling sector. Here, individuals use digital currencies such as Bitcoin, Ethereum, or other alternative coins to participate in diverse gambling activities like casino games, sports betting, lotteries, poker, and beyond. The development of scalable, digitized casino- and crypto-based solutions has supercharged the criminal business environment across Southeast Asia, particularly in the Mekong. Cryptocurrency gambling has become a very common trend in most online casinos. Crypto gambling works the same way as gambling with dollars, pounds, or any other fiat currency - you place your bet and you win or you lose. It’s not a new concept either. Many gaming sites now claim to offer this service. Despite its popularity, only a few people understand how crypto-wagering works.

Here’s an overview of how the process works:

1. Registration: After selecting a suitable crypto casino, players need to open an account. The best Bitcoin casinos simply ask for an email address and password, and possibly a username. This is unlike regular online casinos, which are legally required to collect personal information.
2. Deposits: Players can often choose from a range of popular cryptocurrencies when making a deposit. This typically includes Bitcoin, Ethereum, Tether, Dogecoin, and Litecoin. After selecting a crypto, the casino will display the unique deposit address. Players need to transfer the cryptocurrencies to this address from a private wallet. Payments should be credited in a couple of minutes.
3. Playing Games: Leading crypto casinos offer thousands of games from reputable software providers. This can include slots, table games, live dealers, video poker, and even sports betting. Some crypto casinos also offer ‘provably fair’ games, which are backed by blockchain technology. More on this later.
4. Stakes: Knowing how much you’re staking in cryptocurrencies can be challenging. With this in mind, crypto casinos usually convert stakes to US dollars (or a preferred currency). For instance, instead of staking 0.00023 BTC, you can type in $10.
5. Withdrawals: The biggest benefit of using a crypto casino is that many offer automated withdrawals. You’ll need to provide your crypto wallet address. This is where the casino will transfer the funds. In most cases, the tokens should appear in your private wallet in a few minutes.

5. Findings

Originality/Value- The research enhances our knowledge of the use of virtual currency in both domestic and transnational money laundering activities. The study adds to the emerging literature on how technological advancements facilitate the movement of illegal funds across borders. The paper also presents and evaluates potential strategies for mitigating risks from money laundering activities and provides suggestions for established and emerging financial institutions to implement effective anti-money laundering measures.

6. Conclusion

In conclusion, the cryptocurrency landscape presents both exciting opportunities and significant challenges when it comes to combating money laundering. While methods like mixing, fiat-to-crypto exchanges, privacy-oriented coins, and online gambling offer varying degrees of anonymity and pose challenges to combating money laundering, the inherent transparency of blockchain technology ultimately contributes to revealing illicit activity. Robust safeguards are crucial to harness this transparency effectively. KYC, wallet screening, and transaction monitoring form a vital triad, deterring bad actors through identity verification, risk assessment, and suspicious activity detection. However, balancing these with privacy concerns and agility is necessary. By implementing these tools and fostering collaboration between platforms, regulators, and law enforcement, we can unlock a secure and promising future for cryptocurrency, mitigating the risks and maximizing its potential benefits.

References

1. Albrecht, C., Duffin, K., Hawkins, S., & Rocha, V. (2019). The use of cryptocurrencies in the money laundering process. Journal of Money Laundering Control. https://doi.org/10.1108/JMLC-12-2017-0074.
2. Dyntu, V., & Dykyi, O. (2019). CRYPTOCURRENCY IN THE SYSTEM OF MONEY LAUNDERING. Baltic Journal of Economic Studies. https://doi.org/10.30525/2256-0742/2018-4-5-75-81.
3. Samanta, S., Mohanta, B., Pati, S., & Jena, D. (2019). A Framework to Build User Profile on Cryptocurrency Data for Detection of Money Laundering Activities. 2019 International Conference on Information Technology (ICIT), 425-429. https://doi.org/10.1109/ICIT48102.2019.00081.
4. Yang, L., Dong, X., Xing, S., Zheng, J., Gu, X., & Song, X. (2019). An Abnormal Transaction Detection Mechanism on Bitcoin. 2019 International Conference on Networking and Network Applications (NaNA), 452-457. https://doi.org/10.1109/NaNA.2019.00083.
5. Lal, B., Agarwal, R., & Shukla, S. (2021). Understanding Money Trails of Suspicious Activities in a cryptocurrency-based Blockchain. ArXiv, abs/2108.11818.

Webliography

1. www.cryptonews.com
2. www.chainalysis.com
3. www.financialcrimeacademy.org
4. www.cryptodispensers.com
5. www.incometax.gov.in
6. https://www.dowjones.com
7. https://www.aiaworldwide.com/insights/aml/international-aml-framework/