Scientific Research Publishing

American Journal of Industrial and Business Management, 2025, 15(2), 362-371
https://www.scirp.org/journal/ajibm
ISSN Online: 2164-5175
ISSN Print: 2164-5167

Cryptocurrency and Money Laundering

Francesco Ernesto Alessi Longa

Azteca University, Chalco, Mexico
Email: ceskone@libero.it

How to cite this paper: Longa, F. E. A. (2025). Cryptocurrency and Money Laundering. *American Journal of Industrial and Business Management, 15,* 362-371.
https://doi.org/10.4236/ajibm.2025.152017

Received: January 28, 2025
Accepted: February 22, 2025
Published: February 25, 2025

Abstract

Cryptocurrencies improved the efficiency of traditional financial transactions, decentralized them, and increased access to finance. However, these developments exacerbate their vulnerabilities by making it simpler for criminals and money launderers to evade money laundering laws. This could also imply that criminals exploited a potential gap in existing law and regulation frameworks between jurisdictions, or that they used cryptocurrencies as de facto forms to better conceal illicit sources, making evasion easier through detection across a border or nation. The paper discusses further the involvement of cryptocurrencies in remodeling methodologies related to money laundering by showing their employment at every placement, layering, and integration phase. Furthermore, it has endeavored to address the issues that regulators confront in combating money laundering and similar unlawful acts by exploring mitigation techniques from an international collaborative and technologically creative standpoint. This study aims to provide insight into how digital cryptocurrencies are linked to financial crimes in the ever-changing environment of hazards and legal requirements that accompany their growth and adoption.

Keywords

Cryptocurrencies, Money laundering, Decentralization, Efficiency, Regulatory Gaps

1. Introduction

Cryptocurrencies entered the world of global banking to enable new types of exchanges: more decentralized, secure, and faster. Since Bitcoin's inception in 2009, there has been an increase in cryptocurrency development and usage, with some benefits being decreased transaction costs and greater accessibility. There is also increased privacy, so established financial systems should see jolts of innovation and greater access to new pathways of economic engagement. This exponential growth of cryptocurrencies presents potential challenges, most especially regard-

ing financial crime. Their decentralized and pseudonymous character made them a perfect tool for criminal activities in money laundering. Criminals take advantage of regulatory gaps and difficulties of technology, concealing the source of an illicit payment to provide considerable challenges for law enforcement and regulatory organizations. The paper discusses the linkage of cryptocurrencies with money laundering in the study of digital currencies' role in the facilitation of unlawful operations by considering legislative and technological options to mitigate these dangers (Joksimović et al., 2024; Carucci, 2023).

2. Methodology

This study employs a comparative analysis of international regulatory frameworks, utilizing both qualitative and quantitative data. Key sources include reports from Chainalysis, Europol, the Financial Action Task Force (FATF), and national financial regulators such as FinCEN. The research examines patterns in cryptocurrency-related money laundering, focusing on jurisdictions with both strong and weak AML enforcement. The study also integrates statistical data to assess the effectiveness of different regulatory approaches, providing a balanced discussion of policy implications. By combining descriptive analysis with empirical data, this paper aims to offer a comprehensive perspective on the current challenges and potential solutions in cryptocurrency regulation (Lin et al., 2023).

3. The Relationship Between Cryptocurrency and Money Laundry

The potential of cryptocurrency to transform the financial sector is undeniable. Since the inception of Bitcoin in 2009, many people have used it as a foundation for developing their ideas on advanced blockchain technology. It began as a monetary substitute, but it has now transformed into a tool with many benefits and has become intrinsic in many fields even the illegal sectors such as money laundry. Money laundering refers to concealing illicitly obtained monies to make them appear legitimate. It is a process composed of three stages: placement, layering, and integration, in that order. Cryptocurrencies are new technology with new tools at each stage and therefore create new problems in terms of prevention and detection.

3.1. Placement

Placement is the secret insertion of proceeds of crime through the financial system. In most instances, this process has become easier with the use of virtual currencies, such that illegal money can easily be converted through cryptocurrency exchanges into virtual assets via online intermediaries. Most methods of this kind absolutely bypass established banking networks and organizations in the regulated financial system; therefore, detection becomes all the more problematic. These are some of the factors that, in turn, contribute to a weak regulatory framework or lax enforcement in countries and invite criminals to open businesses where transac-

tions will not come under much scrutiny, making it hard for authorities to detect and intercept such suspicious transactions.

3.2. Layering

Privacy cryptocurrencies, also known as "privacy coins," are a class of cryptocurrencies that has increased anonymity in the entire cycle of issuance, ownership, and transfer of the asset. The two leading and most popular coins in this space are monero and zcash; both have better anonymization techniques than traditional cryptocurrencies. For example, monero deploys advanced obfuscation techniques that mask shrink transaction details, thereby making its privacy framework stronger compared to Bitcoin. Even the level of confidentiality is higher, as it makes tracking the origin of any transaction much more difficult and tracing where the money moves within the system (Almeida et al., 2023).

3.3. Integration

Another critical phase in money laundering is the integration phase, which allows the criminal to legitimize illicit monies by re-injecting them into the economy. Integration has helped criminals in washing off illicitly obtained monies to make them lawful. The integration of cryptocurrencies would imply the digital assets being first converted to cash, and after that, direct consumption of the asset to buy some products or services. The procedures, in turn, followed in placing an order for merchandise at strategically selected places and their delivery to certain addresses do the rest to help in that way. Thus, mixing of coins would be done with relatively lesser costs but also with concealed transactional histories.

3.4. Inherent Features of Cryptocurrencies and Their Appeal for Illicit Activities

A pertinent question arises: What inherent characteristics of cryptocurrencies render them particularly appealing for illicit activities? While the answer is multifaceted, several key factors warrant careful examination.

3.5. Pseudonymity and Anonymity

Pseudonymity is one of the basic properties of cryptocurrencies. The blockchain technology provides a user with the ability to maintain wallet addresses secret, which means anonymity is offered, and that is not typical in traditional financial systems. While the public ledger guarantees transparency, some cryptocurrencies like Monero and Zcash have further enhanced anonymity. Monero uses Ring Signatures which obscure a single transaction by fusing multiple users' signatures to hide the said transaction. Zcash uses Zero-Knowledge Proofs that allow transactions to be verified without reference to the identities of parties or the actual amount of money passed. While these are quite pristine means for safeguarding the rights of the user's privacy, the same attributes allow activities to be carried out flawlessly where malicious parties go unnoticed.

4. Global Reach and Regulatory Challenges

The rise of cryptocurrencies is as much a blessing as it is a curse. It encourages free international trade without the need for third parties. This renders most of the old financial barriers inconsequential, decreasing cost and time to complete any transaction. However, the same absence of physical intermediaries that makes cryptocurrencies so efficient for legitimate global commerce complicates regulatory enforcement. Transactions, though crypto secured against external meddling, are not always spawned out to monitor and track. The degree of oversight in various countries defines the potential for misuse. Indeed, jurisdictions with weak regulatory frameworks are often reported for cryptocurrency-related financial crimes (IMF, 2023).

The best example is when cryptocurrencies are used to evade economic sanctions or for financing transnational criminal organizations. Since these assets are not necessarily related to the mainstream banking systems, they enable criminal actors to overcome certain restrictions that could otherwise bar transactions. However, one should not misunderstand the issue. Technology itself is not the problem but rather the inefficiency of regulatory frameworks and their implementations in ensuring the compliance of standards set for financial security (Consilium Europa, 2023; Ouyang et al., 2024).

5. Decentralization and the Lack of Oversight

Another critical feature that makes them interesting for both legitimate users and illicit actors is their decentralization. Unlike traditional financial institutions, decentralized platforms of operation, such as decentralized exchanges (DEXs), are without a central authority. This enables transactions to take place entirely independent of established regulatory frameworks, thereby making oversight and enforcement a lot more difficult.

Although Know Your Customer and Anti-Money Laundry practices have been adapted by most centralized exchange, usually nobody in these decentralized platforms has ever asked a customer for identification; this is when all kinds of threats regarding the case of misfeasance become critical because the bad guy doing something unlawful from a monetary standpoint may think himself to have seen an excellent avenue to make sure money movement but without identity verification. Decentralized finance, shortly DeFi, was lately developed, which allowed the user to provide and avail of financial services on a peer-to-peer basis. This development further complicates the layers of regulatory intervention.

6. Privacy Enhancement Technology and Anti-Money Laundering Risks

Cryptocurrencies utilize a host of evolving privacy-enhancing technologies (PETs) that further complicate the tracking process. Shielded transactions and stealth addresses are among such features that have been in use with some cryptocurrencies, like Monero and Dash, adding another layer of obfuscation. This makes tracking

exponentially easier for those utilizing advanced privacy techniques to try to remain undetected.

The rapid adoption of such PETs underlines only the growing problem that regulators and law enforcement are having in tracing illicit financial activity. With more cryptocurrency systems allowing privacy, some of the biggest challenges remain with this constantly evolving digital financial landscape: striking a balance without compromising the privacy of financial transparency for users.

7. A Comparative Analysis of Global Regulatory Frameworks Reveals Significant Differences In Effectiveness and Implementation

In the United States, the Financial Crimes Enforcement Network (FinCEN) classifies cryptocurrency exchanges as money service businesses (MSBs), requiring compliance with strict Know Your Customer (KYC) and Anti-Money Laundering (AML) protocols. However, enforcement varies at the state level, leading to inconsistencies in compliance.

The European Union has adopted a more centralized approach with the Fifth and Sixth Anti-Money Laundering Directives (AMLD5 and AMLD6), requiring crypto-asset service providers to register with authorities and enforce AML controls. Additionally, the upcoming Markets in Crypto-Assets (MiCA) framework aims to establish a uniform regulatory structure across member states, potentially enhancing oversight and reducing illicit transactions.

In contrast, Asian regulatory approaches differ widely. Japan enforces one of the most stringent regulatory environments, requiring cryptocurrency exchanges to register with the Financial Services Agency (FSA) and comply with rigorous AML standards. Conversely, China has imposed a complete ban on cryptocurrency transactions, pushing illicit crypto activities underground rather than eliminating them outright. These disparities illustrate the challenge of achieving global regulatory consistency and highlight the need for enhanced international collaboration to address cross-border financial crimes.

Despite these efforts, several gaps remain:

- **Inconsistent enforcement:** Differing national regulations create loopholes that criminals exploit. A lack of standardized global compliance measures contributes to regulatory arbitrage.
- **Challenges in cross-border cooperation:** The global nature of cryptocurrency transactions complicates regulatory oversight. Varying interpretations of AML laws hinder international collaboration.
- **Lack of real-time monitoring:** Current compliance measures lag behind evolving laundering techniques. The integration of blockchain analytics and artificial intelligence (AI) tools remains underutilized in many regulatory environments.

8. The Role of International Cooperation

To address these challenges, global entities such as the Financial Action Task

Force (FATF) have introduced guidelines, including the "Travel Rule," which requires virtual asset service providers (VASPs) to share transaction information. However, implementation remains uneven across jurisdictions, with some nations failing to align their domestic policies with international standards. A key challenge in international cooperation is the lack of legal harmonization between regulatory bodies. For instance, while the European Union enforces strict AML guidelines under AMLD6, certain jurisdictions, particularly in offshore financial centers, continue to provide safe havens for illicit activities. The lack of standardized compliance requirements allows criminals to exploit regulatory loopholes by transferring funds through countries with weaker oversight. Additionally, geopolitical tensions and jurisdictional conflicts between major economies, such as the United States and China, further complicate efforts to establish a unified framework. Cases like the collapse of major crypto exchanges due to poor cross-border coordination highlight the urgent need for enhanced regulatory collaboration and shared intelligence mechanisms. Addressing these disparities requires stronger bilateral agreements and the development of supranational regulatory authorities to oversee compliance across borders. Stronger coordination between governments, financial institutions, and technology firms is necessary to close these regulatory gaps.

9. Case Studies: The Use of Cryptocurrencies in Money Laundering

Several high-publicity cases have been used to show tendencies through which cryptocurrencies use money laundering. Probably the most prominent case would be that of Silk Road, a darknet marketplace that was highly dependent on Bitcoin transactions as means for doing illicit trades, besides concealing financial transactions.

9.1. Silk Road

The infamous darknet marketplace, Silk Road, relied heavily on Bitcoin for illegal trades and money laundering. Given the pseudonymous nature of Bitcoin, buyers and sellers were able to conduct transactions with a minimized possibility of getting detected. Yet, even with the Bitcoin blockchain being so transparent, Silk Road did much more to stay under the noses of law enforcement. One of the main ways in which financial trails were hidden was through the use of tumblers, or mixers—services devised to break the direct link between the source and recipient of funds. By allowing vendors to make use of such mixing mechanisms, Silk Road effectively fragmented transactional links in a way that made the tracing of illicit financial flows extremely difficult. While Bitcoin is based on a public ledger that can be analyzed using block explorers, wallet addresses do not inherently disclose user identities, introducing a layer of anonymity that is often exploited by criminal actors.

Despite the obfuscation techniques, complete anonymity cannot be guaranteed.

While transactions in the blockchain are forever recorded and publicly available, attributing this information to specific individuals can be extremely tricky if advanced privacy-enhancing technologies are used. Therefore, malicious actors continued to exploit Bitcoin and other cryptocurrencies to conduct illegal financial transactions that sometimes implicate service providers for their ignorant roles in money laundering, thus violating relevant AML laws. While it was ultimately dismantled, the closure of Silk Road did not eradicate the greater problem. The rise in decentralized and open-source marketplaces has brought new challenges, as such platforms operate without a central authority to make regulatory intervention and enforcement much more difficult.

9.2. The PlusToken Scam

The PlusToken scam had promised investors billions of dollars through returns from digital asset fraud, laundering several millions in the process through cash transactions via an immense network and trading platforms that took advantage of loopholes in regulation and inconsistencies in jurisdiction. This underlined some very serious weaknesses in the prevailing financial regulations and further brought home the urgent need for much deeper international cooperation in the fight against financial crimes associated with cryptocurrency.

The PlusToken study has highlighted severe weaknesses in the current procedures around the world in fighting crime, especially those related to digital asset laundering. It shows the enormity of the financial crimes involved with cryptocurrency and the discrepancy in enforcement capability across jurisdictions. Layering has been the hallmark of this scheme, a money laundering strategy of distributing illicit funds into minute transactions across a large number of accounts and platforms. Other than the fact that this simply overworks those involved, it greatly complicates the normally straightforward systems of financial tracking, making it near impossible for any authorities to trace and claw back assets.

10. Ransomware Attacks, Cryptocurrency Fraud, and Regulatory Challenges

The Colonial Pipeline ransomware attack underlined the hazardous consequence of cybercriminals seeking cryptocurrency as modes of payment, making it even easier for bad actors to keep below the radar. In this case, though the ransom money seems to have been traced back and recovered, there were some jolting loop holes observed in the process of tracking down and recovering the money. The challenge of tracking the fee payments made with cryptocurrencies-especially when using features that enhance privacy, like anonymity-showcases the limits of current tracking tools. The case of Colonial Pipeline has also shown that the criminals can hide the payments and then convert the ransoms into the banking system, avoiding traditional financial channels and thus avoiding detection. Strong cybersecurity and adherence to AML standards will remain key in combating such attacks and maintaining proper regulation.

The implosion of QuadrigaCX earlier this year really showed what can go wrong when cryptocurrency exchanges self-regulate. Some $190 million of its customers' funds vanished when the Canadian cryptocurrency exchange's founder died without letting anyone know where the key to its cold wallet was; it started to be seen less as a tragic accident, and more as a fraud with additional cover-up after some digging revealed weaknesses in an industry that is very loosely regulated. The incident is an unfortunate reminder of the adverse impacts of the crypto industry sans regulatory standards and strict controls. This development emphatically underlined in bold how there is a dire need for sound regulations that can assure safety for all kinds of digital assets, especially those held at different cryptocurrency exchanges and with other intermediaries.

11. Regulatory Challenges and Evolving Threats

Cryptocurrencies function in a very fragmented regulatory environment where a handful of jurisdictions have painted fairly clear use and enforcement frameworks, while lax practices elsewhere have allowed illicit activities to flourish. A lack of a common regime has created large gaps in enforcement, especially for newer technologies like DeFi and NFT, which further complicate the ability to track and regulate. Yet criminals adapt to newer regulations through continuous method variations trying to evade them using the implicit properties of these technologies anonymity and obfuscation.

Consequently, some regulations to tackle such options include the Know Your Customer and Anti-Money Laundering rules. anti-money laundering laws are including crypto exchanges also in several Jurisdictions. Ensuring due diligence measures on verification should be conducted upon the user, including supervision of suspicious acts. In general, the basic trend remains irregular, inconsistent prosecution that undermines overall the efficiency brought about by such regulation measures. Firms like Chainalysis/CipherTrace develop in-house blockchain analytical tools using advanced technologies able for tracing suspicious transactions tracing fraud recognition. These tools play a major role in improving the capabilities of the authorities to stay ahead of the criminal tactics.

Global collaboration is also needed. Organizations such as the Financial Action Task Force have implemented measures, such the "Travel Rule," which mandates information-sharing across borders for certain transactions. International cooperation is needed to combat crimes that seek to exploit this borderless world of cryptocurrencies.

12. The Need for Empirical Research and Data-Driven Analysis

Many discussions on cryptocurrency-related money laundering rely on case studies rather than quantitative data. This study highlights key statistics:

Chainalysis (2023) estimates that illicit cryptocurrency transactions accounted for approximately $14 billion in 2021, a 79% increase from 2020.

Europol (2021) reports that over 55% of ransomware-related payments are con-

ducted in cryptocurrencies.

The PlusToken Ponzi scheme laundered approximately $2 billion through digital assets before authorities intervened.

A comparative analysis of regulatory effectiveness shows that stricter AML enforcement correlates with lower illicit transaction volumes. Countries with robust compliance measures, such as Japan and the UK, have reported fewer cryptocurrency-related financial crimes compared to jurisdictions with lax oversight.

13. Mitigation Strategies for Cryptocurrency-Related Money Laundering

- **International Regulation:** By establishing uniform laws across the world, it eliminates the loopholes in the present system and stops them from being abused by criminals due to differences between states. Cooperation across borders is very necessary for not allowing the criminals to go away scot-free owing to the deficiencies in the regulation.
- **Technology investment:** Government is supposed to invest resources in developing top-notch technologies dealing with blockchain analytics and AML. Advanced tools will, thus, enable better identification and prevention of malicious activities. Therefore, it is a must that public-private sectors work fast for such tool development.
- **Training Programs:** Specialized training programs on the details of cryptocurrency transactions should be provided to law enforcement officials. This will enhance the agencies' knowledge and technical ability to respond effectively to new emerging threats and criminal methodologies.
- **Collaboration:** Collaboration between governments, financial institutions, technology companies, and cryptocurrency platforms must be constant in terms of sharing information and developing best practices. This would encourage innovation while understanding security concerns and making it difficult for criminals to manipulate weaknesses in the system.

14. Conclusion

Cryptocurrencies showcase both extraordinary opportunity and certain challenge: high returns with opportunities for criminals. To efficiently try to mitigate such illicit uses of the digital assets, a successful regime will link technological innovation and broadened international cooperation to increased oversight through regulation. Further, training for and deployment of technological tools in detection, like those provided via native blockchain capacities proving the source and provenance of transactions, provides a way to protect financial integrity more and promote greater cryptocurrency responsibility globally.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Almeida, H., Pinto, P., & Vilas, A. F. (2023). *A Review on Cryptocurrency Transaction Methods for Money Laundering.* https://arxiv.org/abs/2311.17203 https://doi.org/10.5220/0011993300003494

Carucci, C. (2023). *Anti-Money Laundering in the Age of Cryptocurrencies*. https://www.researchgate.net/publication/385954430_Anti-money_laundering_in_the_age_of_cryptocurrencies https://doi.org/10.36862/eiz-ng010

Chainalysis (2023). *The Crypto Crime Report.* Chainalysis. https://www.chainalysis.com/

Consilium Europa (2023). *Anti-Money Laundering: Council Adopts Rules Which Will Make Crypto-Asset Transfers Traceable*. https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/anti-money-laundering-council-adopts-rules-which-will-make-crypto-asset-transfers-traceable/

Europol (2021). *Cryptocurrencies and Criminal Activities: A Strategic Report.* Europol.

International Monetary Fund (IMF) (2023). *Anti-Money Laundering and Combating the Financing of Terrorism*. https://www.imf.org/en/Topics/Financial-Integrity/amlcft

Joksimović, M., Paunović, M., & Dedjanski, S. (2024). Money Laundering Using Cryptocurrencies. *НОВИ ЕКОНОМИСТ, 18,* 4-10. https://doi.org/10.69781/NOEK202436035

Lin, D., Wu, J., Fu, Q., Yu, Y., Lin, K., Zheng, Z., & Yang, S. (2023). *Towards Understanding Crypto Money Laundering in Web3 through the Lenses of Ethereum Heists*. https://arxiv.org/abs/2305.14748v1

Ouyang, S., Bai, Q. et al. (2024). Bitcoin Money Laundering Detection via Subgraph Contrastive Learning. *Entropy, 26,* 211. https://www.mdpi.com/1099-4300/26/3/211 https://doi.org/10.3390/e26030211