

THE ROLE OF CRYPTOCURRENCIES IN MONEY LAUNDERING: CHALLENGES AND REGULATORY RESPONSES

NISHANI RANAWEERA^{1,2*} 

¹Department of Criminology and Criminal Justice, University of Sri Jayewardenepura, Nugegoda, Sri Lanka. ²School of Global Studies, Thammasat University, Bangkok, Thailand. Email: ranaweera@sjp.ac.lk

Received: 14 April 2024, Revised and Accepted: 27 May 2024

ABSTRACT

This article aims to dissect the complexities surrounding the utilization of cryptocurrencies in money laundering activities within Asian contexts, focusing on the intertwined regulatory challenges. It seeks to unravel how the cultural nuances and economic ambitions in Asia contribute to the proliferation of such activities, spotlighting the unique hurdles these pose to crafting effective regulatory frameworks. Employing a comprehensive literature review as our primary methodology, we delve into a wide array of sources that include case studies, legal reviews, and analyses of existing detection methods. The focus is specifically on Asian countries, providing a regional lens through which to examine the global issue of cryptocurrency-related money laundering. This approach enables a deep dive into cultural, economic, and regulatory aspects specific to Asia that influences these laundering activities. The investigation reveals a complex interplay of factors fueling cryptocurrency-related money laundering in Asia, including a cultural emphasis on wealth accumulation, competitive economic goals, age-based cultural expectations, significant lapses in auditing practices, misuse of charitable donations, and well-networked support systems facilitating illicit activities. These factors not only perpetuate the region's struggle with development but also present substantial obstacles to effective money laundering detection and regulation. The lack of robust auditing mechanisms and the exploitation of philanthropic avenues emerge as significant vulnerabilities, alongside deeply ingrained cultural and economic motivations.

Keywords: Asia, Cryptocurrency, Fear of crime, Financial crime, Money laundering.

© 2024 The Authors. Published by Innovare Academic Sciences Pvt Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>) DOI: <http://dx.doi.org/10.22159/ijss.2024v12i4.51219>. Journal homepage: <https://innovareacademics.in/journals/index.php/ijss>

INTRODUCTION

Money laundering, the process of concealing the origins of illegally obtained money, typically involves three stages: Placement, layering, and integration. The advent of cryptocurrencies has introduced a novel medium for laundering, characterized by enhanced anonymity, and reduced oversight compared to traditional financial systems (Financial Action Task Force [FATF], 2020). The decentralized nature of blockchain technology, which underpins cryptocurrencies, poses significant challenges for regulators and law enforcement agencies trying to trace and prevent illegal financial flows (Brenig *et al.*, 2015). This has become a pressing issue for global financial security, particularly in Asia, where the rapid adoption of digital currencies intersects with diverse regulatory landscapes and cultural attitudes toward wealth (Albrecht *et al.*, 2019).

The primary research question this article seeks to address is: How do the unique socioeconomic and cultural contexts of Asia influence the use of cryptocurrencies in money laundering activities, and what challenges does this pose to regulatory efforts? This question is highly relevant to the Journal of Money Laundering Control audience, which includes scholars, policymakers, and practitioners engaged in the study and prevention of money laundering. Given the journal's focus on developments in investigation, new trends and techniques, and effective compliance management, insights into cryptocurrency-related money laundering within the Asian context can inform targeted strategies for combating these activities.

This article is structured, first, reviewing the nature of cryptocurrencies and their attractiveness for money laundering purposes. Subsequently, case studies highlight how these digital currencies are utilized in laundering activities across Asia, underscoring the cultural and economic drivers behind these actions. Then examine the regulatory challenges presented by cryptocurrencies, focusing on the specific

hurdles encountered in the Asian regulatory environments. Following this, the article proposes solutions and recommendations for enhancing regulatory frameworks to effectively counteract money laundering through cryptocurrencies in Asia.

THE NATURE OF CRYPTOCURRENCIES AND MONEY LAUNDERING

Cryptocurrencies represent a digital or virtual form of currency, utilizing cryptography for security, which makes them difficult to counterfeit. Unlike traditional fiat currencies, cryptocurrencies operate on decentralized platforms, primarily blockchain technology, which records transactions across multiple computers to ensure the integrity and immutability of transaction records (Nakamoto, 2008). This inherent anonymity and the lack of a centralized regulatory authority make cryptocurrencies appealing for money laundering activities (Foley *et al.*, 2019).

MONEY LAUNDERING TRADITIONALLY INVOLVES THREE STAGES

Placement, where illicit funds are introduced into the financial system; layering, where the funds are obscured through a series of transactions to separate them from their origin; and integration, where the funds are reintroduced into the economy as legitimate (Levi and Reuter, 2006). Cryptocurrencies have added a new dimension to this process. The digital nature of these currencies allows for rapid and cross-border transactions, often bypassing traditional monitoring and regulatory mechanisms. Furthermore, the possibility to create and use multiple, pseudonymous digital wallets complicates the tracking of funds, effectively serving the layering stage of money laundering (De Koker and Jentzsch, 2013).

Cryptocurrency-related laundering often involves the use of online exchanges and tumblers, services that mix potentially identifiable or "tainted" cryptocurrency funds with others to obscure the trail back to the fund's original source (Möser *et al.*, 2013). In addition, the

emergence of privacy-focused cryptocurrencies, such as Monero and Zcash, which provide enhanced anonymity features, further complicates the detection of laundering activities (Koerhuis *et al.*, 2020).

Given the complexity and technological sophistication of laundering methods using cryptocurrencies, traditional anti-money laundering (AML) strategies often fall short. The decentralized, borderless nature of cryptocurrencies requires a re-evaluation of existing regulatory frameworks and the development of new detection methodologies that can adapt to the digital landscape (Fama *et al.*, 2019).

CASE STUDIES OF CRYPTOCURRENCY USE IN MONEY LAUNDERING IN ASIA

The PlusToken scam

Background

PlusToken, one of the largest cryptocurrency scams in history, was primarily operated out of China and promised high-yield returns for investors' cryptocurrency deposits. The scheme collapsed in 2019, revealing a Ponzi scheme that affected millions of investors and involved an estimated \$2 billion worth of cryptocurrencies, including Bitcoin, Ethereum, and EOS (Okta, 2023).

Methods used

The operators of PlusToken utilized a classic Ponzi scheme model, paying earlier investors with the new investors' funds. To launder the proceeds, the scammers used a series of complex transactions across multiple cryptocurrencies and exchanges. They also employed coin mixers and moved funds through private wallets to obscure the origins and movements of the illicit funds (Editorial Team, 2023).

Regulatory response

The Chinese authorities arrested several individuals connected to the PlusToken scam in 2020. This case has prompted Chinese regulators to tighten oversight of cryptocurrency exchanges and initial coin offerings to prevent similar scams and laundering activities. It also underscored the need for international cooperation in tracing and seizing cryptocurrency-related illicit assets (Hu, 2023).

North Korean hackers laundering stolen funds

Background

North Korean hacker groups, such as Lazarus, have been implicated in several high-profile cryptocurrency thefts aimed at funding the regime's nuclear and ballistic missile programs. These groups have stolen hundreds of millions of dollars worth of cryptocurrencies from exchanges, notably in South Korea and Japan ("North Korean crypto hackers have stolen \$3B since 2017, says UN Security Council: Report," 2024).

Methods used

The hackers typically gain access to exchange wallets through phishing attacks and malware. After acquiring the cryptocurrencies, they launder the funds through a web of transactions across different exchanges and countries. They use mixers and privacy coins to further obscure the trail. The laundered money is believed to be used for financing the regime's prohibited nuclear and missile programs (Laksono and Nugraha, 2018).

Regulatory response

In response to these incidents, Asian countries, particularly South Korea and Japan, have strengthened their cybersecurity measures and regulatory frameworks around cryptocurrency exchanges. The FATF has also updated its guidelines, urging member countries to adopt more stringent oversight of virtual asset service providers (VASPs) to prevent the misuse of cryptocurrencies by rogue states (FATF, 2019).

These case studies highlight the sophisticated methods used by individuals and state actors in Asia to launder money through cryptocurrencies. They also underscore the challenges faced by

regulators in tracking and preventing such activities, given the borderless and anonymous nature of digital currencies. The regulatory responses have been a mix of stricter domestic measures and enhanced international cooperation, reflecting the global effort required to tackle cryptocurrency-related money laundering.

REGULATORY CHALLENGES AND SOLUTIONS

Regulatory challenges posed by cryptocurrencies

The unique characteristics of cryptocurrencies, including their anonymity, decentralization, and cross-border fluidity, pose significant challenges to traditional AML frameworks. These frameworks were primarily designed for a centralized financial system, where entities such as banks play a key role in monitoring transactions and reporting suspicious activities (European Banking Authority, 2019). Cryptocurrencies bypass these traditional intermediaries, making it difficult for regulatory bodies to track the flow of funds and identify illicit activities.

Furthermore, the rapid evolution of digital currency technologies outpaces the development of regulatory policies, creating a lag in effective governance (FATF, 2020). Jurisdictional variances in cryptocurrency regulation further complicate international efforts to combat money laundering, as launderers can exploit these differences to move illicit funds across borders with relative ease (Bryans, 2014).

Innovations in regulatory approaches

In response to these challenges, regulatory bodies are exploring innovative approaches to enhance AML efforts in the cryptocurrency space. One key strategy is the development of global standards for cryptocurrency regulation. The FATF has issued guidance that includes the "travel rule," which requires VASPs, such as cryptocurrency exchanges, to collect and share information about the parties involved in transactions (FATF, 2020). This aims to extend traditional AML requirements to the cryptocurrency sector, enhancing transparency and traceability of transactions.

National regulators in Asia are also adopting more stringent regulations for cryptocurrency exchanges and wallets. These include mandatory identity verification, known as know your customer (KYC) procedures and the requirement for exchanges to report suspicious transactions to authorities (Kepli and Zuhuda, 2019). For instance, Japan's financial services agency (FSA) has implemented a licensing regimen for cryptocurrency exchanges, which mandates compliance with AML and counter-terrorism financing standards (FSA Japan, 2019).

TECHNOLOGICAL SOLUTIONS TO ENHANCE AML EFFORTS

Advancements in technology are also providing new tools to tackle money laundering in the cryptocurrency domain. Blockchain Analysis software, which can trace the flow of funds on the blockchain, is increasingly being used by law enforcement and regulatory agencies to detect and investigate suspicious activities (Chainalysis, 2020). These tools can identify patterns indicative of money launderings, such as the use of mixers or the rapid movement of funds across multiple wallets and exchanges.

Artificial intelligence (AI) and machine learning are emerging as powerful allies in identifying unusual transaction patterns and potential money laundering activities. By analyzing vast amounts of data, AI can help predict and flag high-risk transactions in real-time, significantly improving the efficiency of AML monitoring systems (Pavlidis, 2023).

The challenges cryptocurrencies pose to AML frameworks require a multifaceted response, combining regulatory innovation, international cooperation, and technological advancements. As regulators in Asia and around the world continue to adapt and refine their approaches, the integration of global standards, stringent oversight, and cutting-edge technology will be crucial in combating money laundering in the digital currency landscape.

FUTURE OUTLOOK AND IMPLICATIONS FOR RESEARCH AND PRACTICE

Evolution of cryptocurrency use in money laundering

The use of cryptocurrencies in money laundering is expected to grow more sophisticated as technologies evolve and digital currencies gain broader acceptance. Privacy-enhancing cryptocurrencies, which offer greater anonymity than Bitcoin, are likely to become more popular among those seeking to launder money, posing additional challenges for detection and regulation. Furthermore, the rise of decentralized finance (DeFi) platforms could create new avenues for laundering, given their ability to facilitate lending, borrowing, and trading without traditional financial intermediaries (Auer and Claessens, 2020).

In Asia, the rapid digitalization of economies and the high adoption rate of cryptocurrencies will likely fuel the increase of such activities. However, this will also push regulators and law enforcement agencies in the region to innovate and adapt more quickly to the changing landscape, potentially leading to more robust and effective regulatory frameworks and enforcement mechanisms.

AREAS FOR FUTURE RESEARCH

Given the evolving nature of cryptocurrency use in money laundering, several areas for future research emerge. One key area is the development of methodologies to trace transactions involving privacy coins and DeFi platforms, which currently pose significant challenges to monitoring and surveillance efforts. In addition, research into the socioeconomic factors that contribute to the prevalence of cryptocurrency-related money laundering in Asia can provide insights into targeted policy interventions.

Another critical area is the impact of regulatory disparities across jurisdictions in Asia on the effectiveness of AML efforts. Comparative studies of regulatory frameworks and their enforcement outcomes can identify best practices and promote harmonization of regulations across the region.

PRACTICAL IMPLICATIONS FOR POLICYMAKERS, LAW ENFORCEMENT, AND FINANCIAL INSTITUTIONS

Policymakers in Asia must consider adopting a dynamic and flexible approach to cryptocurrency regulation that can quickly adapt to technological advancements. This includes engaging with the cryptocurrency industry to develop standards and guidelines that balance innovation with the need to prevent money laundering. For law enforcement, investing in technology and training to enhance digital forensic capabilities are essential for effectively investigating cryptocurrency-related crimes. Collaboration with international bodies and law enforcement agencies in other jurisdictions will also be crucial, given the cross-border nature of these activities. Financial institutions, on the other hand, need to enhance their KYC and AML procedures to address the unique challenges posed by cryptocurrencies. This could involve integrating advanced analytics, AI, and blockchain monitoring tools into their compliance programs to detect suspicious activities more effectively. The landscape of cryptocurrency use in money laundering is rapidly evolving, presenting both challenges and opportunities for research and practice. As the digital economy continues to grow in Asia, the region will play a critical role in shaping the global response to these challenges. By fostering collaboration among policymakers, law enforcement, and the financial sector, and by investing in research and technology, Asia can lead the way in developing innovative solutions to combat cryptocurrency-related money laundering.

CONCLUSION

This article has embarked on a detailed exploration of the role of cryptocurrencies in money laundering, with a specific focus on the Asian context. Through the examination of case studies, regulatory challenges, and the implications for research and practice, several key insights have emerged. First, the inherent features of cryptocurrencies,

such as anonymity and the ability to conduct cross-border transactions swiftly, have significantly facilitated money laundering activities. The case studies of the PlusToken scam and North Korean hackers underscore the sophistication of such activities in Asia and highlight the urgent need for robust regulatory responses and international cooperation. Second, the regulatory landscape in Asia, although rapidly evolving, faces significant challenges in keeping pace with the technological advancements of cryptocurrencies. The adoption of global standards such as the FATF's "travel rule" and the enhancement of national regulations, as seen in Japan and South Korea, represents critical steps forward. However, disparities in regulatory frameworks across jurisdictions remain a considerable hurdle. Innovations in technology, particularly in blockchain analysis and AI, offer promising tools for improving the detection and prevention of cryptocurrency-related money laundering. These technologies have the potential to significantly enhance the capabilities of law enforcement agencies and financial institutions in monitoring suspicious activities.

The future outlook suggests that as cryptocurrencies continue to evolve and integrate into the global financial system, money laundering methods will become increasingly sophisticated. This underscores the importance of continuous research into new regulatory and technological solutions. Specifically, future research should focus on developing methods to trace transactions involving privacy coins and DeFi platforms, understanding the socioeconomic drivers of cryptocurrency-related money laundering in Asia, and assessing the impact of regulatory disparities on the effectiveness of AML efforts. In conclusion, combating cryptocurrency-related money laundering requires a multi-faceted approach that includes dynamic regulatory frameworks, advanced technological tools, and international cooperation. The insights gained from this article contribute to the broader understanding of the challenges and opportunities presented by the rise of cryptocurrencies. By addressing these challenges proactively, policymakers, law enforcement, and financial institutions can better safeguard the integrity of the financial system in the digital age.

ACKNOWLEDGMENT

The author acknowledges Dr. Piyasuda Pangsapa from Thammasat University, Bangkok, Thailand, for her guidance and expertise in the principles and standards of academic writing.

AUTHOR'S CONTRIBUTION

I conceived of the study, collected data, analyzed the data, and wrote the manuscript.

CONFLICTS OF INTEREST

I declare no conflicts of interest concerning this article's research, authorship, and publication.

FUNDING SOURCE

I received no financial support for this article's research, authorship, and publication.

REFERENCES

- Albrecht, C., Duffin, K. M., Hawkins, S., & Morales Rocha, V. M. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*, 22(2), 210-216.
- Auer, R., & Claessens, S. (2018). *Regulating cryptocurrencies: Assessing market reactions*. BIS Quarterly Review. Available from: https://www.bis.org/publ/qrpdf/r_qt2003j.htm
- Brenig, C., Accorsi, R., & Müller, G. (2015). *Economic analysis of cryptocurrency-backed money laundering*. ECIS 2015 Completed Research Papers. Available from: https://aisel.aisnet.org/ecis2015_cr/153
- Bryans, D. (2014). Bitcoin and money laundering: mining for an effective solution. *Indiana Law Journal*, 89(1), 441-472.

- Chainalysis. (2020). *The state of crypto crime*. Available from: <https://www.chainalysis.com/reports/the-state-of-crypto-crime-2020>
- De Koker, L., & Jentzsch, N. (2013). Financial inclusion and financial integrity: Aligned incentives? *World Development*, 44, 267-280.
- Editorial Team. (2023, March). *PlusToken scam: Complete overview. Billion dollar crypto fraud!* Coin Bureau. Available from: <https://www.coinbureau.com/analysis/plustoken-scam>
- European Banking Authority. (2019). *Report with advice for the European Commission on crypto-assets*. Available from: https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2019/646905/EBA%20Report%20with%20advice%20for%20the%20EC%20on%20crypto-assets/882575.pdf
- Fama, M., Fumagalli, A., & Lucarelli, S. (2019). Cryptocurrencies, monetary policy, and new forms of monetary sovereignty. *International Journal of Political Economy*, 48(2), 174-194.
- Financial Action Task Force (FATF). (2019). Guidance for a risk-based approach to virtual assets and virtual asset service providers. Available from: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>
- Financial Action Task Force (FATF). (2020). Guidance for a risk-based approach to virtual assets and virtual asset service providers. Available from: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html>
- Financial Services Agency Japan (FSA Japan). (2019). *Regulation of cryptocurrency in Japan*. Available from: <https://www.fsa.go.jp/en/refer/cryptocurrency/index.html>
- Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, 32(5), 1798-1853.
- Hu, J. (2023). The regulation of cryptocurrency in China. *SSRN Electronic Journal*, <http://dx.doi.org/10.2139/ssrn.4423780>
- Kepli, M. Y., & Zuhuda, S. (2019). Cryptocurrencies and anti-money laundering laws: The need for an integrated approach. In *Emerging issues in Islamic finance law and practice in Malaysia* (pp. 247-263). United Kingdom: Emerald Publishing Limited.
- Koerhuis, W., Kechadi, T., & Le-Khac, N. (2020). Forensic analysis of privacy-oriented cryptocurrencies. *Forensic Science International: Digital Investigation*, 33, 200891.
- Laksono, H. T., & Nugraha, M. F. (2018). Cryptocurrency fever: Should Southeast Asian countries cooperate on facing cryptocurrency market? In: *Proceedings of airlangga conference on international relations*.
- Levi, M., & Reuter, P. (2006). Money laundering. *Crime and Justice*, 34(1), 289-375.
- Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the bitcoin ecosystem. In *Proceedings of the eCrime Researchers Summit (eCRS 2013)*.
- Nakamoto, S. (2008). Bitcoin: *A peer-to-peer electronic cash system*. Available from: <https://bitcoin.org/bitcoin.pdf>
- North Korean crypto hackers have stolen \$3B since 2017, says UN Security Council: Report. (2024, March). CoinDesk: Bitcoin, ethereum, crypto news and price data. Available from: <https://www.coindesk.com/policy/2024/03/21/north-korean-crypto-hackers-have-stolen-3b-since-2017-says-un-security-council-report>
- Okta. (2023, February). The PlusToken cryptocurrency scheme: Architecture and exposure. Employee and Customer Identity Solutions. Okta. Available from: <https://www.okta.com/identity-101/plus-token/#:~:text=The%20PlusToken%20scam%20involved%20cryptocurrency,latest%20victims%20of%20the%20scheme>
- Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: The dawn of a new era. *Journal of Money Laundering Control*, 26(7), 155-166.