

COMBATING CRYPTOCURRENCY LAUNDERING BY ORGANISED CRIME GROUPS THROUGH AN EFFECTIVE REGULATORY FRAMEWORK

Sankul Kabra*

Saira Gori**

ABSTRACT

Money laundering has long been a major issue for governments, law enforcement agencies, and financial institutions around the globe. As technology advances, so too do money laundering methods, presenting new challenges for authorities and financial entities. Organised Crime Groups (OCGs) are increasingly exploiting digital platforms, cryptocurrencies, and virtual assets to disguise illicit funds while maintaining anonymity and complicating their transactions. This article analyses the problem of cryptocurrency laundering by the OCGs and various tactics employed by the OCGs to cover their trails. This article also in-depth discusses the international instruments such as the United Nations Convention against Transnational Organised Crime and Financial Action Task Force recommendations on the prevention of cryptocurrency laundering. The special focus of this paper is on the legal framework regarding cryptocurrency laundering in the United States, European Union and Malaysia. The findings of the paper suggest that there is a regulatory framework present in these jurisdictions but their regulations are not subject specific and regulatory powers have been

* PhD Scholar, Gujarat National Law University, Attalika Avenue, Knowledge Corridor, Koba, Gandhinagar, Gujarat - 382421, India. Email: sankulphd202021@gnlu.ac.in (Corresponding Author).

** Assistant Professor, Gujarat National Law University, Attalika Avenue, Knowledge Corridor, Koba, Gandhinagar Gujarat - 382421, India . Email : s.gori@gnlu.ac.in

[Received: 26 August 2024, Accepted: 6 May 2025, Published: 28 May 2025]



granted to the authorities that are not specialised and skilled to tackle the problem of combating cryptocurrency laundering by OCGs.

Keywords: Cryptocurrencies, Money Laundering, Organised Crime Groups.

MEMERANGI PENGUBAHAN WANG KRIPTO OLEH KUMPULAN JENAYAH TERANCANG MELALUI KERANGKA UNDANG-UNDANG YANG BERKESAN

ABSTRAK

Pengubahan wang haram sudah sekian lama menjadi isu utama bagi kerajaan, agensi penguatkuasaan undang-undang, dan institusi kewangan di seluruh dunia. Seiring dengan kemajuan teknologi, begitu juga kaedah pengubahan wang haram, telah menimbulkan cabaran baharu bagi pihak berkuasa dan entiti kewangan. Kumpulan Jenayah Terancang (OGS) semakin bijak mengeksploitasi platform digital, mata wang kripto, dan aset maya untuk menyembunyikan dana haram dengan mengekalkan ketanpanamaan dan merumitkan transaksi mereka. Artikel ini menganalisa masalah pengubahan wang haram mata wang kripto oleh Kumpulan Jenayah Terancang (OCG) dan pelbagai taktik yang digunakan oleh OCG untuk menutupi jejak mereka. Artikel ini juga membincangkan secara mendalam instrumen antarabangsa seperti Konvensyen Pertubuhan Bangsa-Bangsa Bersatu Menentang Jenayah Terancang Transnasional dan rekomendasi Pasukan Petugas Tindakan Kewangan (FATF) mengenai pencegahan pengubahan wang haram mata wang kripto. Tumpuan khusus kertas kerja ini adalah pada kerangka undang-undang mengenai pengubahan wang haram mata wang kripto di Amerika Syarikat, Kesatuan Eropah dan Malaysia. Dapatan kertas kerja ini mencadangkan bahawa terdapat kerangka undang-undang di dalam bidang kuasa ini tetapi undang-undang ini tidak tertumpu kepada subjek tertentu dan kuasa pengawalseliaan telah diberikan kepada pihak berkuasa yang tidak khusus dan berkemahiran untuk menangani masalah memerangi pengubahan wang haram mata wang kripto oleh OCG.

Kata Kunci: Mata Wang Kripto, Pengubahan Wang Haram, Kumpulan Jenayah Terancang.

INTRODUCTION

In recent years, the rise of cryptocurrencies has transformed the financial landscape, offering unprecedented opportunities for innovation and financial inclusion. However, this technological advancement has also presented new challenges, particularly in the realm of financial crime. One of the most pressing issues is the use of cryptocurrencies for money laundering by organised crime groups (OCGs). Cryptocurrencies are digital assets that utilise cryptographic methods to secure and authenticate transactions and to regulate the issuance of new units. These assets generally function on decentralised systems known as blockchains, which ensure secure and transparent transactions without requiring a central authority such as a bank.¹ When cryptocurrency is transferred, the transaction is logged on the blockchain, which acts as a public ledger maintained and shared by numerous computers globally.² Transactions are validated and processed by a network of users known as “miners”, who receive new cryptocurrency units as compensation for their work.³

Money laundering (ML) has been a persistent global issue for decades. It involves concealing the origins of illegally acquired funds to make them appear legitimate. This practice allows OCGs to benefit from their illicit gains while hiding the financial trail that could lead to their detection and prosecution. Traditionally, ML relied on physical cash transactions and intricate networks of intermediaries. However, the advent of the digital age has transformed financial transactions, introducing new opportunities and challenges for those engaged in money laundering.

¹European Parliament. "Regulation (Eu) 2023/1114 of the European Parliament and of the Council of 31 May 2023." edited by European Parliament: Official Journal of the European Union, (2023).

²Al-Tawil, Tareq Na'el. "Anti-Money Laundering Regulation of Cryptocurrency: UAE and Global Approaches." *Journal of Money Laundering Control* (2022).

³European Council. "Digital Finance: Agreement Reached on European Crypto-Assets Regulation (Mica)." June 30 2022, <https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>.

Organised crime is defined as the commission of serious offenses by a group of individuals working together with the goal of achieving financial or monetary gain. Traditional OCGs typically have intricate structures with established hierarchies and specific roles assigned to each member.⁴ Historically, these groups have received support from local politicians and rely on corrupt practices to avoid problems with law enforcement agencies.⁵ The OCGs often operate in a covert and decentralised manner, with distinct crews or cells responsible for different criminal activities. This compartmentalisation helps keep the group's activities hidden.⁶ The structure of these groups serves to protect them from law enforcement efforts and minimise the risk of infiltration or betrayal.⁷ To ensure a unified understanding of organised crime among member states, the United Nations Convention against Transnational Organised Crime was established. This convention defines an OCG as a "structured group of three or more individuals working together to commit crimes for financial gain, either directly or indirectly".⁸

Cryptocurrencies, with their pseudonymous and decentralised nature, provide a veil of anonymity that can be exploited for illicit activities. The OCGs adept at leveraging sophisticated financial mechanisms, have increasingly turned to digital currencies to obscure the origins of their illicit funds.⁹ By utilising various techniques such as layering, mixing services, and cross-border transactions, these groups can effectively mask their financial activities and evade

⁴Lampe, Klaus Von. "Definitions of Organized Crime." (2019). <http://www.organized-crime.de/organizedcrimedefinitions.htm>.

⁵Greco, Fulvio, and Gianpiero Greco. "Organised Crime: Underground Economy and Regulations to Combat Cybercrime." *European Journal of Political Science Studies*. Vol. 4 Issue (1). (2020) .doi: <https://doi.org/10.46827/ejps.v4i1.935>

⁶Caparini, Marina. UN Police and the challenges of organised crime. Stockholm International Peace Research Institute. (2019)

⁷Leukfeldt, E Rutger, Edward R Kleemans, and Wouter P Stol. "A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists." *Crime, Law and Social Change*, Vol. 67 Issue 1. (2017) 21-37. doi: <https://doi.org/10.1007/s10611-016-9662-2>

⁸United Nations Secretariat. United Nations Convention Against Transnational Organized Crime and the Protocols Thereto. (2005).

⁹Engeler, Sara Maria, and Stefano Baliatti. Cryptocurrencies, Rational Choice, and Organized Crime. (2021)

traditional regulatory and enforcement measures.¹⁰ To combat this growing threat, governments, financial institutions, and regulatory bodies are ramping up their efforts. This involves enhancing regulatory frameworks, improving transaction monitoring systems, and fostering international cooperation. By adopting advanced technologies like blockchain analytics and implementing stricter Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, stakeholders aim to disrupt the financial operations of organised crime and maintain the integrity of the cryptocurrency ecosystem.¹¹

The literature on combating money laundering through cryptocurrencies by the OCGs is very limited, and there are no papers discussing the applicability of international and domestic laws of leading jurisdictions in combating the said problem. This article aims to analyse the problem of money laundering through cryptocurrencies by the OCGs and analyse the legal framework applicable for combating this problem. This paper also throws light on FATF recommendations, International Conventions and analysis of domestic laws in the US, European Union and Malaysia to combat the problem of money laundering through cryptocurrencies by the OCGs. In a first of its kind, this paper analyses international conventions and domestic laws of the US, Europe and Malaysia that can curb the problem of money laundering through cryptocurrencies by the OCGs.

RESEARCH METHODOLOGY

This paper employs a descriptive analytical approach. The study will adopt a multidimensional approach, and examine relevant legislation, scholarly literature, and data to assess measures for combating cryptocurrency laundering by the OCGs. The exploratory research into existing literature i.e. books, journals, articles, etc. shall provide a deeper understanding of the concept, nature and best practices for tackling cryptocurrency laundering. The descriptive analytical

¹⁰Engeler, Sara Maria, and Stefano Balietti. Cryptocurrencies, Rational Choice, and Organized Crime. (2021)

¹¹Al-Tawil, Tareq Na'el. "Anti-Money Laundering Regulation of Cryptocurrency: UAE and Global Approaches." *Journal of Money Laundering Control* (2022).

approach is best suited for the study due to a lack of research on the topic, and no papers throwing light on FATF recommendations, international conventions and domestic laws of the US, Europe and Malaysia regarding the problem of money laundering through cryptocurrencies by the OCGs.

Cryptocurrencies and ML by the OCGs

The scale of ML involving cryptocurrencies is immense. The total value of cryptocurrency received by illicit addresses in 2023 was USD 46.1 billion. In 2024, there was a drop in value received by illicit addresses to USD 40.9 billion. However, the data for 2024 is preliminary and the data could easily surpass the USD 51 billion mark.¹² Cryptocurrencies were partially designed to reduce transaction costs, a feature evident in their various built-in characteristics. While some argue that cryptocurrencies involve high information and control costs, it is generally true that cryptocurrency transactions are cheaper and faster than those conducted with fiat currencies due to the absence of intermediaries between buyers and sellers.¹³ However, these same features have also been exploited by the OCGs for ML. Specifically, three aspects of cryptocurrencies significantly reduce transaction costs for such illicit activities.

Firstly, cryptocurrencies' decentralised structure allows users to transfer value directly to each other without the involvement of third parties. As discussed earlier, traditional anti-money laundering measures often focus on monitoring intermediaries who facilitate transactions to prevent illicit transfers.¹⁴ The absence of intermediaries in cryptocurrencies disrupts this approach, and the lack of face-to-face

¹²Chainalysis. "2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized." (2025) <https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/>.

¹³Zakarneh, Shadi Khaled, Zaer Qaroush, and Ammar Dawabsheh. "Cryptocurrencies advantages and disadvantages: a review." *International Journal of Applied Sciences and Smart Technologies* Vol. 4 Issue 1.1-20. (2022)

¹⁴Budish, Eric B. "Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains." *University of Chicago, Becker Friedman Institute for Economics Working Paper* (2022).

interaction in cryptocurrency transactions further complicates the process of identifying the parties involved.¹⁵ Secondly, although every transaction is recorded and traceable on the blockchain, there is no direct link to the individuals or organisations behind those transactions. Cryptocurrencies operate in a pseudonymous environment, where only the public key, an arbitrary sequence of numbers, is visible, while the private key remains concealed.

This makes it extremely challenging to associate a real-life identity with a cryptocurrency's address.¹⁶ For instance, person X is assigned "xxxxbb2234" as a public key, and he sends 0.5 Bitcoin to person Y, who has a public key as "yyyyaa5566". The blockchain will record that 0.5 Bitcoin was transferred from xxxxbb2234 to yyyyaa5566, but those particular public keys belong to person X and Y will not be known to anyone. Therefore, KYC regulations, discussed in the later part of the paper, become important to associate a public key/information with a particular real life person. Additionally, users can easily create multiple electronic wallets, each with different public addresses, complicating investigations into potential money laundering activities.¹⁷

Lastly, Cryptocurrencies' transaction speed and ease of use offer significant advantages over traditional methods of money laundering, such as cash. Unlike physical paper money, which has limitations related to weight and size, cryptocurrencies can be stored in large quantities on a simple USB device and transferred to anyone worldwide within minutes. The flexible nature of cryptocurrency transactions also facilitates the evasion of regulatory measures by allowing users to divide a large transaction into smaller ones.¹⁸

¹⁵Zakarneh, Shadi Khaled, Zaer Qaroush, and Ammar Dawabsheh. "Cryptocurrencies advantages and disadvantages: a review." *International Journal of Applied Sciences and Smart Technologies* Vol. 4 Issue 1.1-20. (2022)

¹⁶Kabra, Sankul, and Saira Gori. 2023. "Drug trafficking on cryptomarkets and the role of organized crime groups." *Journal of Economic Criminology* 2:100026.

¹⁷Budish, Eric B. "Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains." *University of Chicago, Becker Friedman Institute for Economics Working Paper* (2022).

¹⁸Nuryyev, Guych, David W Savitski, and John E Peterson. "The

ML plays a crucial role for OCGs engaged in trafficking activities on cryptomarkets. These groups produce large amounts of cryptocurrencies, which they convert into cash. To disguise the illegal origin of these funds, they must launder the money, making it appear as if it were earned legitimately. This process often involves a convoluted series of financial transactions, moving money across various accounts and jurisdictions, which complicates the tracing of the funds' origins. ML enables the OCGs to continue their illicit operations and conceal the profits derived from drug trafficking.¹⁹ The OCGs on the dark web are adept at laundering cryptocurrencies, which can be quickly moved between accounts and are challenging to trace.²⁰ These groups often employ "professional enablers" such as lawyers, accountants, and bankers to obscure their illicit funds.

The OCGs sometimes hold onto the cryptocurrencies they receive from cryptomarket transactions as investments. These crypto assets are used to finance other illegal activities, both online and offline.²¹ Cryptocurrencies not retained as investments are laundered and integrated into the legitimate economy. For example, Dutch law enforcement discovered that a cryptomarket moderator used his connections to exchange bitcoins for physical cash.²² In April 2023, an Indian gang leader was sentenced to eight years and ten months in prison for drug trafficking through online channels on EncroChat and

microeconomics of cryptocurrencies." *The Economics of Cryptocurrencies*. (2020).

¹⁹Gilmour, Paul Michael. "Reexamining the anti-money-laundering framework: a legal critique and new approach to combating money laundering." *Journal of Financial Crime*. (2022) doi: <https://doi.org/10.1108/jfc-02-2022-0041>

²⁰Budish, Eric B. "Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains." *University of Chicago, Becker Friedman Institute for Economics Working Paper* (2022).

²¹Greco, Fulvio, and Gianpiero Greco. "Organised Crime: Underground Economy and Regulations to Combat Cybercrime." *European Journal of Political Science Studies*. Vol. 4 Issue (1). (2020) .doi: <https://doi.org/10.46827/ejps.v4i1.935>

²²Kruisbergen, Edwin W, Eric R Leukfeldt, Edward R Kleemans, and Robert A Roks. "Money talks money laundering choices of organized crime offenders in a digital age." *Journal of Crime and Justice* Vol. 42 Issue 5. (2019). 569-581. doi: <https://doi.org/10.1080/0735648x.2019.1692420>

admitted to money laundering charges in the United Kingdom's Guilford Crown Court.²³

In East and Southeast Asia, Point running syndicates, or 'moving ants,' are a significant tool for ML, leveraging numerous individuals, often unemployed youth, who provide their bank accounts and create front companies to obscure the origins and destinations of stolen funds.²⁴ These operations involve routing money through various bank or cryptocurrency accounts and online casinos, where it is disguised as legitimate casino winnings.²⁵

Motorcades, a more sophisticated evolution of point running, utilise advanced layering techniques to further complicate the money trail, often collaborating across multiple groups to handle substantial transactions more efficiently.²⁶ This complex system poses significant challenges for detection and investigation due to the volume of transactions and the cross-border nature of the schemes, necessitating enhanced financial transparency, improved international cooperation, and stronger regulatory frameworks to effectively combat these illicit activities.²⁷

²³PTI. 2023. "Indian-origin man in UK jailed for drug smuggling, money laundering." *India Today*, April 30, 2023. <https://www.indiatoday.in/world/story/indian-origin-man-uk-money-laundering-drug-smuggling-jailed-2366455-2023-04-30>.

²⁴United Nations Office on Drugs and Crime. *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*. (2024).

²⁵United Nations Office on Drugs and Crime. *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*. (2024).

²⁶Nimma, Sudarshan. "Money Laundering in the Cyberworld: Emerging Trends." *Part 1 Indian J. Integrated Rsch. L.* Vol. 2 Issue 1. (2022).

²⁷United Nations Office on Drugs and Crime. *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*. (2024).

As authorities have deepened their understanding of third- and fourth-party payments, particularly following initiatives like 'Operation Chain Break' and similar efforts in China,²⁸ the OCGs have increasingly turned to cryptocurrencies for their illegal gambling activities, creating significant challenges for investigators.²⁹ In the Philippines, licensed casinos and junket operators were found to be heavily involved in laundering approximately USD81 million stolen in a 2016 cyberattack linked to the Lazarus Group from the Bangladesh Central Bank.³⁰

Although the funds initially passed through banks and remittance firms, they were untraceable after reaching the casino junket operators.³¹ The emergence of cyberspace and cryptocurrencies has opened a new front for the OCGs involved in illicit markets such as drugs, arms, human trafficking, and sexual exploitation.³² The DEA alleges that global drug cartels have used Binance, the largest cryptocurrency exchange, to launder millions of dollars, with transactions ranging between \$15 million and \$40 million.³³ Binance is reportedly cooperating with investigators as it faces scrutiny over these allegations.

²⁸Nimma, Sudarshan. "Money Laundering in the Cyberworld: Emerging Trends." *Part 1 Indian J. Integrated Rsch. L.* Vol. 2 Issue 1. (2022).

²⁹Langdale, John. "Money laundering in Australian casinos." *Journal of Money Laundering Control* Vol. 26. Issue 7. (2023). 99-109. doi: <https://doi.org/10.1108/JMLC-09-2022-0136>.

³⁰Langdale, John. "Money laundering in Australian casinos." *Journal of Money Laundering Control* Vol. 26. Issue 7. (2023). 99-109. doi: <https://doi.org/10.1108/JMLC-09-2022-0136>.

³¹Nimma, Sudarshan. "Money Laundering in the Cyberworld: Emerging Trends." *Part 1 Indian J. Integrated Rsch. L.* Vol. 2 Issue 1. (2022).

³²Paula, Ebberth L, Marcelo Ladeira, Rommel N Carvalho, and Thiago Marzagão. "Deep learning anomaly detection as support fraud investigation in brazilian exports and anti-money laundering." 15th IEEE International conference on machine learning and applications. (2016).

³³Yusoff, Yusri Hazrol, Nur Ain Fatihah Azlan, Nurfarahin Nisa Mohd Zamzuri, Nurfarhin Sufian, Sarah Nadya Rudy Kurniawan, and Razinah Hassan. "Areas of Technology That Helps in Combating Money Laundering: A Concept Paper." *Journal of Academic Research in Business and Social Sciences* Vol. 13 Issue 5. (2023). 949-959. doi: <https://doi.org/10.6007/IJARBS/v13-i5/16588>.

The OCGs employ various techniques to launder the cryptocurrencies. The widely used methods are discussed below:

Smurfing

There is a significant increase in transactions that fall just below the USD 1,000, 3,000, and 10,000 thresholds. These amounts correspond to various regulatory reporting requirements, suggesting that some individuals may be structuring their payments to evade further scrutiny. This practice, known as 'smurfing' in traditional finance, seems to have been adapted to the cryptocurrency realm.³⁴

Intermediary Wallets

A key technique used in cryptocurrency-based money laundering is the employment of intermediary wallets. This 'layering' strategy aims to conceal the link between illegal funds and their eventual integration into the legitimate financial system. The number of such intermediary wallets has surged dramatically.³⁵ In 2023, over 1.4 million intermediary wallets were involved in moving known illicit funds, a significant rise from approximately 800,000 in 2022.³⁶ This increase suggests that the OCGs are employing more advanced methods to avoid detection, creating more intricate networks of wallets to hide the movement of illicit funds.

Notably, the use of multiple intermediary wallets by illicit actors is growing more rapidly on exchanges with KYC verification processes

³⁴Kolachala, Kartick, Ecem Simsek, Mohammed Ababneh, and Roopa Vishwanathan. "SoK: money laundering in cryptocurrencies." Proceedings of the 16th International Conference on Availability, Reliability and Security. (2021).

³⁵Kolachala, Kartick, Ecem Simsek, Mohammed Ababneh, and Roopa Vishwanathan. "SoK: money laundering in cryptocurrencies." Proceedings of the 16th International Conference on Availability, Reliability and Security. (2021).

³⁶Devanesan, Johanan. "Understanding Crypto Money Laundering, and How to Get a Handle on It." Fintech News. (2024). <https://fintechnews.sg/98478/crypto/understanding-crypto-money-laundering-and-how-to-get-a-handle-on-it/#:~:text=The%20proliferation%20of%20intermediary%20wallets%20has%20been%20remarkable.,a%20substantial%20increase%20from%20about%20800%2C000%20in%202022.>

compared to those without such requirements. This pattern suggests that money launderers may be refining their strategies to avoid detection on platforms with stringent verification, possibly by using numerous wallets to fragment their activities and circumvent detection.

Consolidation Wallets

The use of consolidation wallets, which gather and merge funds from multiple sources, is a notable trend to monitor. In 2024, the top 100 bitcoin consolidation wallets accumulated £968 million in bitcoin from over 14,970 separate addresses.³⁷ Broadening the view, more than 1,500 consolidation wallets received a combined total of £2.6 billion in bitcoin throughout 2024, with each wallet collecting funds from at least ten different sources.³⁸ This consolidation pattern may suggest efforts to obscure the origin of funds prior to transferring them to exchanges or other cash-out destinations.³⁹

Mixing Services, Privacy Coins and Bridges

Mixers, or tumblers, have experienced varying levels of popularity as tools for money laundering. These services combine cryptocurrencies from multiple users, complicating efforts to trace the origins of the funds. Examples include CoinJoin, Wasabi Wallet, and Join Market.⁴⁰ The use of mixers hit a high in 2022, with over USD1.5 billion processed in April alone.⁴¹

³⁷Chainalysis. "2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized." (2025)

³⁸Chainalysis. "2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized." (2025)

³⁹Zhou, Fangfang, Yunpeng Chen, Chunyao Zhu, Lijia Jiang, Xincheng Liao, Zengsheng Zhong, Xiaohui Chen, Yi Chen, and Ying Zhao. "Visual analysis of money laundering in cryptocurrency exchange." *IEEE Transactions on Computational Social Systems*. Vol. 11. Issue 1. (2024). 731-745.

⁴⁰Wronka, Christoph. "Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures." *Journal of Money Laundering Control*. Vol. 25. Issue. 1. (2022). 79-94.

⁴¹Chainalysis. "2025 Crypto Crime Trends: Illicit Volumes Portend Record

Although their use declined due to regulatory actions, some mixers, such as Tornado Cash, have seen a resurgence in 2024, indicating that OCGs are adapting to increased regulatory scrutiny.⁴² Privacy coins, particularly Monero, have gained traction among individuals aiming to evade detection. Monero transactions have increased consistently, with a significant surge in March 2024 due to a spam attack known as Black Marble.⁴³

The strong anonymity features of privacy coins make them particularly appealing to the OCGs, creating substantial challenges for law enforcement and compliance professionals.⁴⁴ Crypto bridges, which enable the transfer of assets between various blockchain networks, have become more frequently used for money laundering.

In January 2024, nearly USD 234 million in illicit funds were recorded moving through these bridges, marking the highest amount to date. This trend underscores how the OCGs are taking advantage of the interoperability between different blockchain networks to further conceal the movement of illicit funds.⁴⁵

Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized." (2025)

⁴²Chainalysis. "2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized." (2025), 31

⁴³Chainalysis. "2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized." (2025)

⁴⁴Chainalysis. "2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized." (2025)

⁴⁵Chainalysis. "2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized." (2025)

Darknet Marketplaces

Darknet marketplaces are hidden online platforms accessed through specialised software such as Tor, which allow for anonymous transactions using cryptocurrencies.

These marketplaces support the exchange of illegal goods and services, providing a means for money launderers to convert illicit funds into cryptocurrencies and vice versa.⁴⁶

Similar to money laundering with fiat currencies, it is challenging to determine the exact amount of money laundered through cryptocurrencies. Agencies such as the FBI, the European Banking Authority, and the Financial Action Task Force of the G7 recognise cryptocurrencies' involvement in money laundering but lack concrete data on the extent of the problem.⁴⁷

Silk Road was a notorious darknet marketplace operating on the Tor network, which allowed for anonymous transactions using cryptocurrencies. Founded in 2011 by Ross Ulbricht, who used the alias "Dread Pirate Roberts," Silk Road became infamous for facilitating the trade of illegal goods and services.

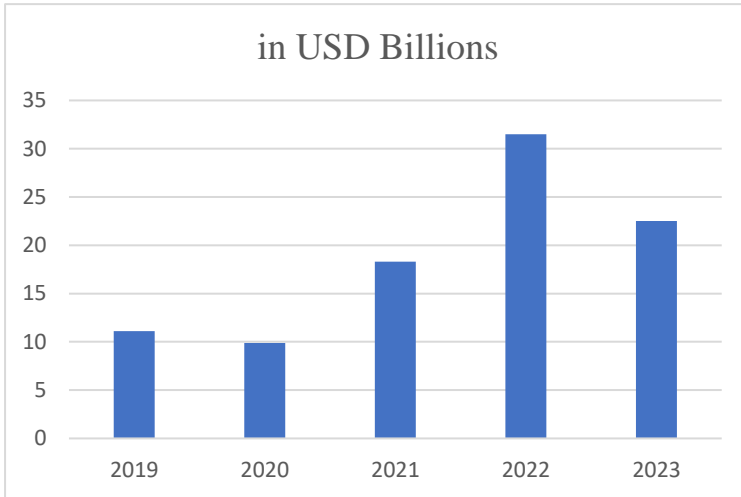
Despite its efforts to remain hidden, it was seized by the FBI in 2013, and Ulbricht was subsequently convicted on multiple charges. The case highlighted the challenges of regulating and policing the dark web and underscored the need for a comprehensive approach to combat digital money laundering.⁴⁸

⁴⁶Bertola, Federico. "Drug trafficking on Darkmarkets: How cryptomarkets are changing drug global trade and the role of organized crime." *American Journal of Qualitative Research* Vol. 4. Issue. 2. (2020). 27-34. doi: <https://doi.org/10.29333/ajqr/8243>

⁴⁷Bertola, Federico. "Drug trafficking on Darkmarkets: How cryptomarkets are changing drug global trade and the role of organized crime."

⁴⁸Chainalysis. "2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized." (2025)

The cryptocurrency laundered from 2019 to 2023 is shown below:⁴⁹



Between 2019 and 2023, the amount of cryptocurrency laundered, exhibited a dynamic trend, starting at USD 11.1 billion in 2019 before slightly decreasing to USD 9.9 billion in 2020. This initial stability was followed by a significant surge, with the laundered amount more than tripling to a peak of USD 31.5 billion in 2022. However, 2023 witnessed a substantial decline to USD 22.5 billion, although this figure remained higher than the levels observed in the earlier years. Considering the huge amount of cryptocurrency laundering, it is important to analyse the applicable legal framework to combat ‘crypto laundering’ by the OCGs.

⁴⁹Chainalysis. "Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group." (2024). <https://www.chainalysis.com/blog/2024-crypto-money-laundering/>.

Legal Frameworks to Combat ‘Crypto-Laundering’ by OCGs

The legal frameworks surrounding cryptocurrencies vary widely across different countries, reflecting a range of approaches from strict prohibition to open encouragement. An endeavour has been made through United Nations Convention against Transnational Organised Crime (UNTOC) to address the transnational organised crime.

United Nations Convention against Transnational Organised Crime

The UNTOC adopted in 2000, is a comprehensive international legal framework aimed at addressing the challenges posed by transnational organised crime. It provides a set of tools for countries to adopt policies and legal measures that can help combat various forms of organised crime, including money laundering related to cryptocurrencies.⁵⁰ This convention is particularly important in the context of cryptocurrency laundering as digital currencies increasingly play a role in illicit financial activities. The UNTOC can significantly aid in the fight against cryptocurrency laundering by encouraging stronger legal frameworks, international cooperation, and the implementation of common standards for dealing with illicit cryptocurrency transactions.⁵¹

Article 1, 13, 16 and 18 provide for Cross-Border cooperation for mutual legal assistance, extradition, and information sharing. Since cryptocurrency transactions can span multiple jurisdictions, UNTOC’s emphasis on international cooperation is critical for tracing and prosecuting criminals using cryptocurrencies for illicit purposes. For instance, the UK’s National Crime Agency (NCA) has taken down a massive, multi-billion-dollar money laundering operation, known as “Operation Destabilise”.⁵² This network catered to a diverse clientele

⁵⁰Boister, Neil. "The cooperation provisions of the UN Convention against Transnational Organised Crime: a ‘toolbox’ rarely used?" *International Criminal Law Review*. Vol. 16. Issue 1. (2016). 39-70.

⁵¹Boister, Neil. "The cooperation provisions of the UN Convention against Transnational Organised Crime: a ‘toolbox’ rarely used?"

⁵²Chainalysis. 2024. "NCA Disrupts Multi-Billion Dollar Russian Money Laundering Network, OFAC Sanctions Related Individuals and Entities." (2024) <https://www.chainalysis.com/blog/nca-disrupts-multi-billion-dollar-russian-money-laundering-network-2024/>.

of criminals, including wealthy Russians, international power players, cybercriminals, and drug trafficking organizations. The NCA pinpointed two Russian-speaking groups, “Smart” and “TGR”, as the masterminds behind these activities. So far, their investigation has resulted in 84 arrests and the seizure of over 20 million Euros in cash and digital currencies.⁵³ This successful disruption was a joint effort of signatories to the convention, including the UK’s Metropolitan Police Service, France’s Direction Centrale de la Police Judiciaire, the US Treasury’s Office of Foreign Assets Control, the Drug Enforcement Agency, and the Federal Bureau of Investigation.⁵⁴

The UNTOC in Article 34 encourages nations to adopt consistent legal measures for combating money laundering, which is essential for managing the growing risks of cryptocurrency-related financial crimes. For instance, Financial Action Task Force (FATF) mandates KYC and Customer Due Diligence practices to detect and report suspicious cryptocurrency transactions, which are applicable to all countries irrespective of their domestic legislations.⁵⁵ The UNTOC fosters the development of international standards, helping countries adopt stronger cybersecurity and investigative tools to detect illicit cryptocurrency activities.⁵⁶ For example, UNTOC’s information-sharing mechanisms help EU law enforcement agencies, such as Europol, to collaborate in tracking illicit cryptocurrency transactions. This can also involve Eurojust, the EU agency for judicial cooperation, which ensures effective prosecution across borders.

In conclusion, the UNTOC provides a vital global framework for combating cryptocurrency laundering by promoting international

⁵³TRM Labs. "US DOJ Brings Charges In \$230 Million Crypto-Laundering Case." (2024) <https://www.trmlabs.com/resources/blog/us-doj-brings-charges-in-230-million-crypto-laundering-case>.

⁵⁴TRM Labs. "US DOJ Brings Charges In \$230 Million Crypto-Laundering Case." (2024) <https://www.trmlabs.com/resources/blog/us-doj-brings-charges-in-230-million-crypto-laundering-case>.

⁵⁵FATF. Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs. (2023)

⁵⁶Tennant, Ian, and Ana Paula Oliveira. "Applying the right lessons from the negotiation and implementation of the UNTOC and the UNCAC to the implementation of the newly agreed UN ‘cybercrime treaty.’" *Journal of Cyber Policy*. (2024). 1-18.

cooperation, legal harmonisation, and capacity building in law enforcement.

Recommendations by Financial Action Task Force

The FATF has established a comprehensive set of standards to combat money laundering and terrorist financing, and these standards explicitly address virtual assets (including cryptocurrencies) and virtual asset service providers (VASPs).⁵⁷ The FATF provides clear definitions for “virtual assets” and “virtual asset service providers” to ensure consistent application of its standards. Virtual Asset is defined as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. VASP includes any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of activities such as exchange between virtual assets and fiat currencies; exchange between one or more other forms of virtual assets; transfer of virtual assets; safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets and participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset.⁵⁸

Recommendation 15 specifically addresses virtual assets. It states that countries should assess and mitigate the ML risks associated with virtual asset activities and VASPs. The FATF mandates that VASPs should undertake Customer Due Diligence (CDD), record keeping, Suspicious Transaction Reporting (STR), Internal Controls and Compliance Programs and Sanctions Screening.⁵⁹ Recommendation 16: requires VASPs to obtain, hold, and transmit originator and beneficiary information for virtual asset transfers that exceed a certain threshold (currently USD/EUR 1,000). This is often referred as the “Travel Rule”. This rule aims to prevent the use of virtual assets for illicit purposes by ensuring transparency in transactions. It requires VASPs to exchange this information with

⁵⁷FATF. Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs. (2023)

⁵⁸FATF. Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs. (2023)

⁵⁹FATF. Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs. (2023)

counterparty VASPs or other obliged entities. The implementation of the Travel Rule for virtual assets has been a significant focus for the FATF, and it continues to urge countries to effectively implement and enforce it.⁶⁰

The FATF regularly updates its guidance on virtual assets to reflect the evolving risks and technological developments in the cryptocurrency space. Countries are expected to implement these standards into their national laws and regulations. The FATF continues to monitor the implementation of these standards globally and encourages jurisdictions to prioritise their effective enforcement.⁶¹

United States

In the U.S., the regulatory landscape for cryptocurrencies is multifaceted, involving multiple federal and state agencies. The Securities and Exchange Commission regulates securities and has classified many cryptocurrencies and Initial Coin Offerings (ICOs) as securities. In *SEC v. DAO*, it has been held that cryptocurrencies are securities and therefore, they are bound by SEC regulations.⁶² The Commodity Futures Trading Commission treats Bitcoin and other cryptocurrencies as commodities and oversees derivatives and futures markets related to these assets.⁶³ Financial Crimes Enforcement Network (FinCEN) regulates cryptocurrency exchanges and wallet providers as money transmitters, requiring them to comply with AML and KYC regulations. Internal Revenue Service treats cryptocurrencies as property for tax purposes, meaning that gains and losses are subject to capital gains tax.⁶⁴ Regulation is often decentralised, with states like New York having their own specific frameworks, such as the

⁶⁰FATF. Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs. (2023)

⁶¹FATF. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. (2021).

⁶²Filimonov, Ihor. "Cryptocurrency Regulation: A Comparative Analysis of the European Union and the United States." Central European University. (2024).

⁶³Filimonov, Ihor. "Cryptocurrency Regulation: A Comparative Analysis of the European Union and the United States."

⁶⁴Filimonov, Ihor. "Cryptocurrency Regulation: A Comparative Analysis of the European Union and the United States."

BitLicense, while others have more lenient or undefined policies. The BitLicense is a business license that requires traders to adhere to more rigorous AML standards. In California, regulations require Bitcoin traders to maintain bank-like reserves to cover potential losses, while North Carolina is still working on proposed Bitcoin regulation bills and currently has no directives in effect.⁶⁵

The US Attorney launched a criminal prosecution against Rule and Nysewander, who were accused of working with others to disguise the illegal profits from online romance scams, business email compromises, real estate scams, and other frauds by using cryptocurrency.⁶⁶ They allegedly converted the stolen money into cryptocurrency and sent it to accounts managed by their associates both in the U.S. and abroad. Furthermore, when opening accounts and communicating with banks and cryptocurrency exchanges, Rule and Nysewander are said to have provided false information and concealed important details. Over the course of this alleged scheme, they and their co-conspirators are accused of laundering over USD 2.4 million. Both these accused were convicted and could face up to 20 years in federal prison for each money laundering count.⁶⁷ Similarly, in August 2024, indictment was brought against Lam and Serrano for crypto-theft of USD 230 million.⁶⁸

US prosecutors have also shown an iron fist to Binance, the company running the largest global cryptocurrency exchange, Binance.com. The company admitted guilt today and will pay more than USD 4 billion to settle the Justice Department's investigation into violations of the Bank Secrecy Act (BSA), not registering as a money transmitter, and the International Emergency Economic Powers Act (IEEPA).⁶⁹ Changpeng Zhao, Binance's Canadian founder and former

⁶⁵Filimonov, Ihor. "Cryptocurrency Regulation: A Comparative Analysis of the European Union and the United States."

⁶⁶United States Attorney's Office. Montana man convicted in cryptocurrency money laundering conspiracy. (2025).

⁶⁷ United States Attorney's Office. Montana man convicted in cryptocurrency money laundering conspiracy. (2025).

⁶⁸TRM Labs. "US DOJ Brings Charges In \$230 Million Crypto-Laundering Case." (2024) <https://www.trmlabs.com/resources/blog/us-doj-brings-charges-in-230-million-crypto-laundering-case>.

⁶⁹US Department of Justice. Binance and CEO Plead Guilty to Federal Charges in \$4B Resolution. (2023).

CEO, also pleaded guilty to failing to implement an adequate anti-money laundering (AML) program, which violated the BSA. As part of the plea agreement, Zhao has stepped down as CEO of Binance.⁷⁰

Though prosecutors have been able to successfully prosecute money launderers and cryptocurrency exchanges, there needs to be a clearer, safer cryptocurrency market for eager investors, regulators could establish more detailed regulations specifically designed for the crypto industry.⁷¹ Just as the rise of e-commerce decades ago spurred legislative efforts resulting in the Framework for Global Electronic Commerce, the current revolutionary nature of cryptocurrency and its various forms necessitates similar guidance. Providing specific rules for sales involving particular coins and crypto funds could offer much-needed clarity.⁷² Without a more developed regulatory framework, relying solely on enforcement actions by bodies like the SEC is insufficient to achieve their regulatory objectives. Ultimately, these enforcement actions can negatively impact the very investors the SEC aims to protect and hinder involvement in potentially beneficial companies. Among the proposed legislation targeting cryptocurrency is the Digital Asset Anti Money Laundering bill, which seeks to curb money laundering and other criminal activities associated with cryptocurrency by focusing on parties involved in transactions, such as miners and validators.⁷³

European Union

Currently, the EU has not implemented a unified legal framework for crypto-assets that applies across all member countries. However, the EU Commission has put forward several proposals such as the Sixth Anti-Money Laundering Directive (6AMLD), which would require businesses dealing in crypto-assets to register with national authorities,

⁷⁰US Department of Justice. Binance and CEO Plead Guilty to Federal Charges in \$4B Resolution. (2023).

⁷¹Joseph Steinbach. "An Analysis of the Current U.S. Regulatory Framework Surrounding Cryptocurrency." *Northeastern University Law Review*. (2024).

⁷²Joseph Steinbach. "An Analysis of the Current U.S. Regulatory Framework Surrounding Cryptocurrency."

⁷³Joseph Steinbach. "An Analysis of the Current U.S. Regulatory Framework Surrounding Cryptocurrency."

follow anti-money laundering rules, and report any suspicious transactions. The aim of 6AMLD is to close loopholes in the individual laws of EU countries by creating consistent definitions for money laundering and virtual assets throughout the EU.⁷⁴

To create a consistent way of regulating crypto-asset operations across the European Union, the European Commission developed the Regulation of the European Parliament and the Council on Crypto-asset Markets and Amending Directive. This set of rules, called MiCA, aims to establish a supervisory structure for crypto-assets, including regulations for those who issue them, service providers, and participants in the secondary market. Making use of these MiCA and 6AMLD, on September 19, 2024, the German Federal Criminal Police dismantled the operational systems of 47 Russian-language cryptocurrency exchanges that did not require identity verification (no-KYC). This operation, known as "Operation Final Exchange," is notable for its extensive reach and for highlighting the critical role that instant-swap, no-KYC exchanges play in enabling online cybercrime.⁷⁵ As the name implies, these no-KYC exchanges do not have any apparent procedures for collecting customer identification details before allowing deposits or withdrawals of any amount. They do not ask for names, phone numbers, or email addresses, and they make no effort to verify any such information before processing transactions.⁷⁶

A key weakness in the current regulatory landscape for crypto-assets is the absence of a central authority with the specific power to oversee and examine crypto-asset transactions. Giving the responsibility of supervising and regulating cryptocurrencies to bodies that do not specialise in this area diminishes the impact of these regulations. Furthermore, a significant issue within the crypto-legal framework is the absence of clear guidelines and prerequisites for obtaining licenses to conduct activities involving crypto-asset transactions.⁷⁷

⁷⁴Filimonov, Ihor. "Cryptocurrency Regulation: A Comparative Analysis of the European Union and the United States."

⁷⁵Chainalysis. "In Large Operation, German Law Enforcement Seizes Servers of 47 Russia-centric No KYC Exchanges." (2024).

⁷⁶Chainalysis. "In Large Operation, German Law Enforcement Seizes Servers of 47 Russia-centric No KYC Exchanges." (2024).

⁷⁷Benson, Vladlena, Bogdan Adamyk, Anitha Chinnaswamy, and Oksana

Malaysia

Combating cryptocurrency laundering in Malaysia involves a combination of legal frameworks and regulatory policies aimed at curbing money laundering using cryptocurrencies. Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 is Malaysia's primary legislation for combating money laundering and terrorism financing. The Act includes provisions to prevent the laundering of proceeds from unlawful activities, including those derived from the use of cryptocurrencies.⁷⁸

The Securities Commission (SC) is the key regulator for the cryptocurrency and digital asset industry in Malaysia. In 2019, the SC issued guidelines on Digital Assets to regulate ICOs, cryptocurrency exchanges, and digital asset transactions. These guidelines include the requirement for exchanges to comply with AML measures. The SC also regulates Security Token Offerings to prevent illicit activities in the digital asset space.⁷⁹ These guidelines classify specific digital currencies and tokens as securities. This action brings these digital assets under the authority of the SC, which means cryptocurrency businesses face more compliance requirements, such as needing to obtain licenses to operate legally. Those who organise coin offerings without the necessary registration could be imprisoned for up to 10 years or fined up to 10 million Malaysian ringgit (around USD 2.5 million).⁸⁰ In 2021, the SC incorporated the crypto "Travel Rule" requirements into Malaysia's national regulations. This was achieved

Adamyk. "Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions." *European Journal of Law and Economics*. Vol. 57. Issue 1. (2024). 37-61.

⁷⁸Sobri, Mohamad Amerzan Mohamad, and Muneer Ali Abdul Rab. "Regulatory Frameworks for Crypto Assets: Comparative Study Between Malaysia and Indonesia." SALAM Digest: Syariah and Law Undergraduate Symposium. (2024).

⁷⁹Sobri, Mohamad Amerzan Mohamad, and Muneer Ali Abdul Rab. "Regulatory Frameworks for Crypto Assets: Comparative Study Between Malaysia and Indonesia."

⁸⁰Segeenkov, Andrey. "Legal Status Of Cryptocurrencies In Malaysia." *Forbes.com*. (2024) <https://www.forbes.com/sites/digital-assets/2024/09/30/legal-status-of-cryptocurrencies-in-malaysia/>.

by amending the Guidelines on Prevention of Money Laundering and Terrorism Financing for Reporting Institutions in the Capital Market.⁸¹

The legal standing of cryptocurrency in Malaysia was examined in the unreported court case of *Luno Pte Ltd & Anor v Robert Ong Thien Cheng*. In this instance, the plaintiffs, who ran a digital currency exchange, had a customer as the defendant. Due to a technical error, the plaintiffs mistakenly sent the defendant 22.6 Bitcoins instead of the intended 11.3 Bitcoins to his third-party e-wallet. After realising the mistake, the plaintiffs asked for the extra 11.3 Bitcoins back, but the defendant ignored their request. Consequently, the plaintiffs sued the defendant to recover the 11.3 Bitcoins or its equivalent monetary value.⁸² In the initial court ruling, the defendant was ordered to return the 11.3 Bitcoins or its value in Malaysian Ringgit to the plaintiffs. This decision was upheld by the Sessions Court judge on appeal, and the High Court subsequently dismissed a further appeal. A key principle established by this first cryptocurrency case in Malaysia is that while Bitcoin and other digital currencies are not legal tender in the country, they are considered a form of commodity because they are bought using real money. Furthermore, the court ruled that cryptocurrency trading is not illegal, as it is regulated by the SC. Despite this current legal stance, the case is now awaiting a decision at the Court of Appeal.⁸³

According to the Malaysian Ministry of Finance, the use of cryptocurrency for money laundering in Malaysia is currently not widespread. The government's approach to regulating cryptocurrency involves requiring all registered digital asset exchange operators to comply with reporting obligations under the Act of 2001.⁸⁴ Analysing

⁸¹Notabene. "Crypto Travel Rule Regulations in Malaysia by Securities Commission Malaysia (SCM)." (2023). <https://notabene.id/world/malaysia>.

⁸²Ismail Nawang, Nazli, and Ida Madieha. "Cryptocurrency: An Insight into the Malaysian Regulatory Approach." *Psychology and Education Journal*. (2020). doi: 10.17762/pae.v58i2.2319.

⁸³Ismail Nawang, Nazli, and Ida Madieha. "Cryptocurrency: An Insight into the Malaysian Regulatory Approach." *Psychology and Education Journal*. (2020). doi: 10.17762/pae.v58i2.2319.

⁸⁴The Star. "MoF: Low instances of using cryptocurrency in money laundering." *The Star*. (2024) <https://www.thestar.com.my/business/business-news/2024/12/18/mof->

the aforesaid recommendations of FATF in context of the Malaysian legal landscape, the regulatory framework in Malaysia incorporates AML standards, KYC norms, Travel Rule and is therefore, compliant with the FATF recommendations.

CONCLUSION AND THE WAY AHEAD

Addressing the issue of cryptocurrency laundering by the OCGs is a complex and ongoing challenge that requires a multi-layered strategy combining technological advancements, regulatory improvements, and industry cooperation. Cryptocurrencies present unique opportunities for laundering illicit funds due to their pseudonymous nature and the global, decentralised nature of blockchain technology. The OCGs exploit these features through sophisticated laundering techniques including smurfing (breaking down large transactions into smaller ones), using intermediary and consolidation wallets to obfuscate transaction trails, and leveraging mixing services, privacy coins, and bridges to further conceal their activities. Darknet marketplaces also play a critical role in facilitating these operations by providing platforms for anonymous transactions.

Specific regulations are necessary to define market participant parameters and create a framework for investigators to address bad actors.⁸⁵ Techniques such as crypto-tracing, tactical surveillance, and analysis of financial and tax information should be employed as well. Cutting-edge transaction monitoring systems are essential in combating money laundering. There is a significant increase in the use of blockchain analytics tools, with Chainalysis Crypto Compliance solutions screening transactions rising from under 200 million in 2018 to more than 1.4 billion in 2024. These tools employ machine learning and artificial intelligence to identify suspicious patterns that suggest money laundering, delivering real-time alerts to compliance teams.⁸⁶

low-instances-of-using-cryptocurrency-in-money-laundering.

⁸⁵Benson, Vladlena, Bogdan Adamyk, Anitha Chinnaswamy, and Oksana Adamyk. "Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions." *European Journal of Law and Economics*. Vol. 57. Issue 1. (2024). 37-61.

⁸⁶Benson, Vladlena, Bogdan Adamyk, Anitha Chinnaswamy, and Oksana

There has to be Public-Private collaboration to break OCGs, networks and combat the emerging threats can also enhance the effectiveness of AML efforts. Combating cryptocurrency laundering requires collaboration among various stakeholders, including financial institutions, regulatory bodies, technology providers, and law enforcement agencies. A united approach ensures that efforts are not duplicated and that resources are efficiently utilised. Sharing intelligence and best practices can also help in developing more effective strategies for detecting and preventing crypto-laundering activities.

The research indicates that while regulatory frameworks for cryptocurrencies exist in the examined jurisdictions, these regulations often lack specific focus on the unique characteristics and risks associated with digital assets. Consequently, the authority to oversee and enforce these regulations has frequently been assigned to bodies that do not possess the specialised knowledge and skills necessary to effectively combat the complex issue of cryptocurrency laundering by the OCGs. This mismatch between the nature of the threat and the expertise of the regulatory bodies may hinder the efficacy of current measures in preventing and prosecuting cryptocurrency-related money laundering activities. The lack of subject-specific regulations means that crucial nuances of cryptocurrency transactions and the methods employed by the OCGs might not be adequately addressed, while entrusting oversight to non-specialised authorities can lead to challenges in understanding the technical complexities, identifying sophisticated laundering schemes, and implementing targeted enforcement strategies.

In conclusion, the fight against cryptocurrency laundering by the OCGs is ongoing and requires a comprehensive strategy. By leveraging advanced technology, implementing adaptive regulatory measures, and adhering to industry best practices, we can enhance our ability to detect and prevent these illicit activities. The success of these efforts relies on a collaborative and proactive approach that addresses both current and emerging challenges in the cryptocurrency landscape.

Adamyk. "Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions." *European Journal of Law and Economics*

References

- Al-Tawil, Tareq Na'el. "Anti-Money Laundering Regulation of Cryptocurrency: Uae and Global Approaches." *Journal of Money Laundering Control* (2022).
- Bartsch, Robert. 2020. "The relationship of drug and human trafficking and their facilitation via Cryptomarkets and the Dark Web: A recommendation for cryptocurrency regulation."
- Benson, Vladlena, Bogdan Adamyk, Anitha Chinnaswamy, and Oksana Adamyk. 2024. "Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions." *European Journal of Law and Economics* 57 (1):37-61.
- Bertola, Federico. 2020. "Drug trafficking on Darkmarkets: How cryptomarkets are changing drug global trade and the role of organized crime." *American Journal of Qualitative Research* 4 (2):27-34. doi: <https://doi.org/10.29333/ajqr/8243>
- Boister, Neil. 2016. "The cooperation provisions of the UN Convention against Transnational Organised Crime: a 'toolbox' rarely used?" *International Criminal Law Review* 16 (1):39-70.
- Budish, Eric B. 2022. "Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains." *University of Chicago, Becker Friedman Institute for Economics Working Paper* (83).
- Caparini, Marina. 2019. UN Police and the challenges of organised crime. Stockholm International Peace Research Institute.
- Chainalysis. 2025. "2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized." <https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/>.
- Chainalysis. 2024. "Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group." <https://www.chainalysis.com/blog/2024-crypto-money-laundering/>.

- Chainalysis. 2024. "NCA Disrupts Multi-Billion Dollar Russian Money Laundering Network, OFAC Sanctions Related Individuals and Entities." <https://www.chainalysis.com/blog/nca-disrupts-multi-billion-dollar-russian-money-laundering-network-2024/>.
- Chainalysis. 2024. "In Large Operation, German Law Enforcement Seizes Servers of 47 Russia-centric No KYC Exchanges."
- Engeler, Sara Maria, and Stefano Balietti. 2021. *Cryptocurrencies, Rational Choice, and Organized Crime*.
- European Council. "Digital Finance: Agreement Reached on European Crypto-Assets Regulation (Mica)." news release, 30 June 2022, 2022, <https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>.
- European Parliament. "Regulation (Eu) 2023/1114 of the European Parliament and of the Council Pf 31 May 2023." edited by European Parliament: Official Journal of the European Union, 2023.
- Filimonov, Ihor. 2024. "Cryptocurrency Regulation: A Comparative Analysis of the European Union and the United States." Central European University.
- Gilmour, Paul Michael. 2022. "Reexamining the anti-money-laundering framework: a legal critique and new approach to combating money laundering." *Journal of Financial Crime*. doi: <https://doi.org/10.1108/jfc-02-2022-0041>
- Greco, Fulvio, and Gianpiero Greco. 2020. "Organised Crime: Underground Economy and Regulations to Combat Cybercrime." *European Journal of Political Science Studies* 4 (1). doi: <https://doi.org/10.46827/ejps.v4i1.935>
- Ibrahim, Rahmeh Fawaz, Aseel Mohammad Elian, and Mohammed Ababneh. 2021. "Illicit account detection in the ethereum blockchain using machine learning." 2021 international conference on information technology (ICIT).
- Jailani, Muhammad Arief, and Aishath Muneeza. 2023. "Crypto assets: the need for Shariah screening criteria for digital assets in

- Malaysia." *International Journal of Islamic Economics and Finance Research* (1):27-47.
- Kamišalić, Aida, Renata Kramberger, and Iztok Fister Jr. 2021. "Synergy of blockchain technology and data mining techniques for anomaly detection." *Applied Sciences* 11 (17):7987.
- Kolachala, Kartick, Ecem Simsek, Mohammed Ababneh, and Roopa Vishwanathan. 2021. "SoK: money laundering in cryptocurrencies." Proceedings of the 16th International Conference on Availability, Reliability and Security.
- Kreminskyi, Oleh, Olena Kuzmenko, Anastasiia Antoniuk, and Olha Smahlo. 2021. "International cooperation in the investigation of economic crimes related to cryptocurrency circulation." *Studies of Applied Economics* 39 (6).
- Kruisbergen, Edwin W, Eric R Leukfeldt, Edward R Kleemans, and Robert A Roks. 2019. "Money talks money laundering choices of organized crime offenders in a digital age." *Journal of Crime and Justice* 42 (5):569-581. doi: <https://doi.org/10.1080/0735648x.2019.1692420>
- Lampe, Klaus Von. 2019. "Definitions of Organized Crime." accessed 1 Mar. 2023. <http://www.organized-crime.de/organizedcrimedefinitions.htm>.
- Langdale, John. 2023. "Money laundering in Australian casinos." *Journal of Money Laundering Control* 26 (7):99-109. doi: <https://doi.org/10.1108/JMLC-09-2022-0136>.
- Leukfeldt, E Rutger, Edward R Kleemans, and Wouter P Stol. 2017. "A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists." *Crime, Law and Social Change* 67 (1):21-37. doi: <https://doi.org/10.1007/s10611-016-9662-2>
- Levi, Mike, and Melvin Soudijn. 2020. "Understanding the laundering of organized crime money." *Crime and Justice* 49 (1):579-631.
- Longa, Francesco Ernesto Alessi. 2025. "Cryptocurrency and Money Laundering." *American Journal of Industrial and Business Management* 15 (2):362-371.

- Lorenz, Joana, Maria Inês Silva, David Aparício, João Tiago Ascensão, and Pedro Bizarro. 2020. "Machine learning methods to detect money laundering in the bitcoin blockchain in the presence of label scarcity." Proceedings of the first ACM international conference on AI in finance.
- Motamed, Amir Pasha, and Behnam Bahrak. 2019. "Quantitative analysis of cryptocurrencies transaction graph." *Applied Network Science* 4:1-21.
- Nimma, Sudarshan. 2022. "Money Laundering in the Cyberworld: Emerging Trends." *Part 1 Indian J. Integrated Rsch. L.* 2:1.
- Nuryyev, Guych, David W Savitski, and John E Peterson. 2020. "The microeconomics of cryptocurrencies." In *The Economics of Cryptocurrencies*, 35-42. Routledge.
- Paesano, Federico. 2023. "Following the Virtual Money: Investigating Crypto-Based Money Laundering and Confiscating Virtual Assets." In *Cryptocurrency Concepts, Technology, And Applications*, 119-139. Auerbach Publications.
- Paula, Ebberth L, Marcelo Ladeira, Rommel N Carvalho, and Thiago Marzagão. 2016. "Deep learning anomaly detection as support fraud investigation in brazilian exports and anti-money laundering." 2016 15th iee international conference on machine learning and applications (icmla).
- Pettersson Ruiz, Eric. 2021. Combating money laundering with machine learning: A study on different supervised-learning algorithms and their applicability at Swedish cryptocurrency exchanges.
- PTI. 2023. "Indian-origin man in UK jailed for drug smuggling, money laundering." *India Today*, 30 April 2023. <https://www.indiatoday.in/world/story/indian-origin-man-uk-money-laundering-drug-smuggling-jailed-2366455-2023-04-30>.
- Sobri, Mohamad Amerzan Mohamad, and Muneer Ali Abdul Rab. 2024. "Regulatory Frameworks for Crypto Assets: Comparative Study Between Malaysia and Indonesia." SALAM Digest: Syariah and Law Undergraduate Symposium.

- Tang, Zichen, E Haihong, Mingzhi Sun, Lamei Zhao, Rongrong Wang, and Meina Song. 2023. "Anti-money laundering method based on hierarchical risk control knowledge graph." Fifth International Conference on Artificial Intelligence and Computer Science (AICS 2023).
- Tennant, Ian, and Ana Paula Oliveira. 2024. "Applying the right lessons from the negotiation and implementation of the UNTOC and the UNCAC to the implementation of the newly agreed UN 'cybercrime'treaty." *Journal of Cyber Policy*:1-18.
- United Nations Office on Drugs and Crime. 2024. *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*.
- United Nations Office on Drugs and Crime. 2024. *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*.
- United Nations Secretariat. 2005. *United Nations Convention Against Transnational Organized Crime and the Protocols Thereto*.
- Weber, Mark, Giacomo Domeniconi, Jie Chen, Daniel Karl I Weidele, Claudio Bellei, Tom Robinson, and Charles E Leiserson. 2019. "Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics." *arXiv preprint arXiv:1908.02591*.
- Wronka, Christoph. 2022. "Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures." *Journal of Money Laundering Control* 25 (1):79-94.
- Yusoff, Yusri Hazrol, Nur Ain Fatihah Azlan, Nurfarahin Nisa Mohd Zamzuri, Nurfarhin Sufian, Sarah Nadya Rudy Kurniawan, and Razinah Hassan. 2023. "Areas of Technology That Helps in Combating Money Laundering: A Concept Paper." *Journal of Academic Research in Business and Social Sciences* 13 (5):949-959. doi: <https://doi.org/10.6007/IJARBS/v13-i5/16588>.

Zakarneh, Shadi Khaled, Zaer Qaroush, and Ammar Dawabsheh. 2022. "Cryptocurrencies advantages and disadvantages: a review." *International Journal of Applied Sciences and Smart Technologies* 4 (1):1-20.

Zhou, Fangfang, Yunpeng Chen, Chunyao Zhu, Lijia Jiang, Xincheng Liao, Zengsheng Zhong, Xiaohui Chen, Yi Chen, and Ying Zhao. 2024. "Visual analysis of money laundering in cryptocurrency exchange." *IEEE Transactions on Computational Social Systems* 11 (1):731-745.