International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Anonymity Unmasked: The Role of Cryptocurrencies in Global Money Laundering

CA Srushti Mantri

Director of Forensic Accounting, Cube Collaborators Inc., Mukeshkumar Jain & Co., Chartered Accountants

Abstract

This research paper examines the intersection of cryptocurrencies and financial crime, particularly focusing on money laundering. It examines how these digital assets are employed in illicit financial activities, investigates the methodologies used to obscure transaction trails, evaluates regulatory responses to these risks, and presents practical case studies highlighting the real-world criminal use of cryptocurrency. The study, covering data from 2020 to 2024, combines a thorough review of existing literature with empirical analysis of blockchain transactions and case studies.

The novelty of this study is the use of blockchain analysis methods for monitoring cryptocurrency transactions in the blockchain and detecting criminal money laundering techniques. It also examines how the criminals use mixers to exponentially expand the transaction trail and hide the money flow.

Our analysis reveals that cryptocurrencies are often viewed as tools for anonymity but the underlying technology provides tracking of transactions, albeit with challenges, particularly when advanced techniques such as coin mixers, privacy coins, and decentralized exchanges are used. Case studies, including high-profile hacks, highlight the complexities of tracing illicit funds and challenges faced by law enforcement agencies. Despite efforts by global regulatory bodies, regulations on digital assets vary significantly around the world, allowing criminals to exploit jurisdictions with lax regulations for their illicit activities.

The study concludes that cryptocurrencies pose notable risks of money laundering, advancement in digital forensic tools, enhanced regulatory measures, and greater international cooperation are essential to address these risks. This research contributes to the understanding of money laundering through cryptocurrencies and underscores the need for continuous improvement of regulation and technology to ensure finance remains safe in the age of innovation.

Keywords: Cryptocurrency, Money Laundering, Blockchain, Financial Crimes, Digital Forensics, Cryptocurrency Tracking

1. Introduction

Money has always been more than just a medium of exchange; it's a reflection of society's values, power structures, and aspirations. As Niall Ferguson astutely observes in *"The Ascent of Money: A Financial History of the World"*, "Behind each great historical phenomenon, there lies a financial secret", suggesting that the true forces driving pivotal moments in history often reside in the hidden mechanisms of money and finance. This notion rings true today as we confront the complexities of the modern world and observe the rise of a new kind of money: Cryptocurrencies. Born from a desire for greater freedom

and privacy, these digital currencies have captured the imagination of many who see them as a way to escape the control of traditional financial systems. For these enthusiasts, cryptocurrencies symbolize a bold step toward a more autonomous and equitable financial future. However, not everyone shares this enthusiasm. Critics argue that these currencies are fraught with risks, often painting them as tools for frauds and criminal activities. As society grapples with these divergent views, one thing is clear—cryptocurrencies are more than just a passing trend; they represent a profound shift in how we think about money and its place in our lives.

Considering the evolution of money, it is essential to recognize that cryptocurrencies are digital assets operating outside the purview of government financial authorities. This lack of regulation introduces significant risks, including heightened financial insecurity, increased susceptibility to fraud, and a proliferation of financial crimes. With the total market capitalization of $2.36 Trillion, cryptocurrencies have grown to rival the economic output of many countries. In fact, only the top ten countries by GDP exceed this market capitalization. For instance, as of recent data, the GDP of countries such as Russia ($2.06 trillion), Mexico ($2.02 trillion), Australia ($1.79 trillion) and other countries are significantly less than the total market capitalization of cryptocurrencies. This comparison highlights the growing influence of cryptocurrencies in the global financial landscape and underscores their potential for misuse in illicit activities and financial crimes. The gravity of these issues is further emphasized by the fact that the G20 Finance Ministers and Central Bank Governors (FMCBG) addressed them at their meeting in Marrakech, Morocco, on October 13, 2023 and adopted a new regulatory roadmap for crypto assets specifically recommending implementation of Financial Action Task Force (FATF) 2019 standards for virtual asset service providers (VASPs) which are designed to bolster protections against money laundering, terrorist financing, and weapons proliferation.

Given the significant impact of cryptocurrencies on the global financial landscape and the complexities involved in tracking illicit financial flows estimating the scale of such activities remains challenging. Chainalysis Crypto Crime Report 2024 estimated annual outflow of $24.20 billion in crypto crimes, highlighting the substantial financial risks. This research paper delves into the extensive literature and practical studies that explore the relationship between digital currencies and financial crimes, particularly money laundering. Key studies include analyses of the methods used to obscure transaction trails, evaluations of regulatory responses to these risks, and case studies highlighting the real-world impact of cryptocurrency-related crimes. Additionally, practical research conducted by Financial Action Task Force (FATF), Policy Department for Citizens' Rights and Constitutional Affairs, Chainalysis, United Nations Office on Drugs and Crime (UNODC) and Bank for International Settlements has shed light on the vulnerabilities within the cryptocurrency ecosystem and the effectiveness of existing regulations.

This research examines how cryptocurrencies facilitate money laundering, focusing on their methods and operational strategies. Key questions include: How are cryptocurrencies utilized to facilitate money laundering and terrorist financing? What specific methods are employed to obscure transactions within blockchain networks? To what extent are current regulatory frameworks effective in addressing these risks? Additionally, the study will investigate practical aspects such as the tracing of public ledger transactions, use of mixers and other modus operandi adopted by money launderers.

The rest of paper is structured as follows: Section II provides a comprehensive analysis of existing research on cryptocurrencies and their role in illicit activities focusing on anonymity mechanisms, facilitation of money laundering, and global regulatory responses. This review synthesizes theoretical

insights from recent academic papers and reports an to establish a foundational understanding. Section III outlines the research design and approach used in this study including examination of academic and regulatory sources and describes our practical investigations. Section IV presents the findings from both the literature review and our practical studies, highlighting key patterns in cryptocurrency-facilitated money laundering, evaluating regulatory effectiveness, and identifies challenges faced by law enforcement. Section V concludes the paper.

2. Literature Review

The literature on cryptocurrencies and their role in financial crimes is extensive, yet it continues to evolve as new developments emerge. A comprehensive set of studies highlights how cryptocurrencies, due to their decentralized and pseudonymous nature, are increasingly used to facilitate money laundering. Studies such as those by U.S. Department of Homeland Security (2022), Policy Department for Citizens' Rights and Constitutional Affairs (2018), Aryan Kasera in International Journal of Engineering and Advanced Technology (2020), emphasize on anonymity provided by cryptocurrencies and identifies their use in financial crimes and money laundering due to their ability to bypass traditional financial systems. Research has also focused on the specific methods employed to obscure illicit transactions. Elliptic (2020), Pakki, J., Shoshitaishvili, Y., Wang, R., Bao, T., Doup´E, A., & Arizona State University. (2021) identifies the use of mixers such as Helix, Mixcoin, TumbleBit, Obscuro and emerging use of privacy wallets such as Wasabi, Electrum, Mercuryo as a money laundering vehicle. United Nations Office on Drugs and Crime (UNODC) (2022), Financial Crime Academy (2024) studies reflect the use of Peer-to-peer (P2P) networks and over-the-counter (OTC) brokers to facilitate transactions beyond conventional systems. P2P networks enable direct transactions between users with minimal identification requirements, on the other hand, OTC brokers specialize in large-scale trades, offer a degree of discretion and privacy that can be misused to handle significant amounts of money discreetly. Reports from Financial Intelligence Centre (2024), Europol's Internet Organised Crime Threat Assessment (IOCTA) (2024) explains the strategy to have money mules transfer funds for the launderers. Money mules are individuals who allow their bank accounts to be used for purchasing cryptocurrency, thereby obscuring the source of illicit funds and creating a buffer between the criminals and their illegally obtained assets. Vladlen Benson, Umut Turksen, Bogdan Adamyk (2023), U.S. Department of Treasury (2023), Bruegel (2023) highlighted the use of multiple DApps to layer the proceeds of crime thought automated smart contracts, least restrictions on user identities thereby adding more complexities to trace funds. The Elliptic (2023) reports that criminal and high-risk entities have used decentralized exchanges cross-chain bridges, and coin swap services to obscure over $7 billion in illegal cryptocurrency proceeds since 2020. There are various studies from Stokes (2012), Barone and Masciandaro (2019), Dupuis and Gleason (2019) assessing the laundering risks in the era of cryptocurrencies as well as the availability of crime fighting tools in Fintech. In 2019, the Financial Action Task Force (FATF) published updated recommendations referred to as the "Travel Rule" in relation to VAs transfers. In line with the concerns highlighted in our research, the Governor of the Reserve Bank of India, Mr. Shaktikanta Das, articulated a critical perspective at the World Economic Forum in Davos (2024). He stated, "Some celebrate this as a new party, but they forget the crash a few years ago. Volatility, money laundering, and terror financing risks are inherent in these assets." These challenges, as Mr. Das pointed out, are key to grasp wider impact of digital currencies on the global financial system. The European Parliament study on "Virtual currencies and terrorist financing:

assessing risk and evaluating response" highlights legal and regulatory mechanisms, guidance for a risk based approach and various innovative approaches on regulations of cryptocurrencies across Europe.
While considerable research has been conducted on the general use of cryptocurrencies in financial crime, there is a need for more focused studies on the specific challenges of regulating privacy coins and decentralized finance (DeFi) platforms. It should be noted that evidence of money laundering through cryptocurrency remains limited.

3. Methodology

While anonymity complicates the identification of individuals, the use of cryptocurrencies adds another layer of complexity in holding specific persons accountable for money laundering activities. To address this challenge, this research adopts a multi-faceted approach that leverages open-source information, analyzing blockchain transaction patterns, use of mixers and evaluation of case studies involving cryptocurrency-related money laundering to dissect the mechanisms by which cryptocurrencies are utilized in illicit activities. While the literature review section provided foundational definitions and highlighted key studies, it is essential to further contextualize these studies in the broader scope of financial crimes.

Global Estimates of Illicit Cryptocurrency Transactions

According to a 2024 report by Chainalysis, illicit addresses sent $22.2 billion worth of cryptocurrency to services which is a significant decrease from the $31.5 billion sent in 2022. Some of this decline might be linked to a general reduction in cryptocurrency transaction volume, encompassing both legitimate and illicit activities.

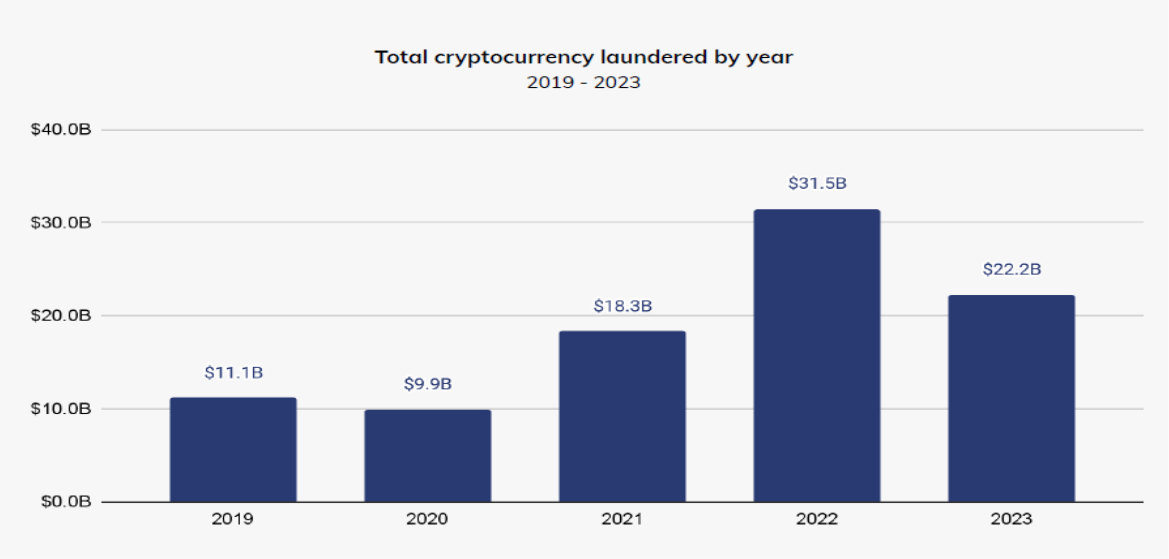

Figure 1: Chainalysis Crypto Crime Report @ 2024 – Total cryptocurrency laundered year by year

This also examines the concentration of illicit funds; the following table provides a comparative of the number of deposit addresses receiving substantial amounts of illicit funds and the total value of these transactions across the years 2022 and 2023.

Year	Number of Deposit Addresses Receiving Over $10M in Illicit Crypto	Total Illicit Crypto Received by These Addresses (in $B)	Number of Deposit Addresses Receiving Over $1M in Illicit Crypto	Total Illicit Crypto Received by These Addresses (in $B)	Percentage of Total Illicit Value Received by Exchanges
2022	40	$2.0B	542	$6.3B	Over 50%
2023	109	$3.4B	1,425	$6.7B	46%

This data reflects an evolving landscape of illicit cryptocurrency transactions, where criminals are increasingly using more addresses to distribute their funds, potentially as a strategy to avoid detection and enforcement efforts.

Techniques and Tactics Employed in Crypto Money Laundering

Various researches also documented the progression of money laundering techniques. Early methods, such as simple peer-to-peer (P2P) exchanges, have evolved into more sophisticated strategies. A report from the Financial Action Task Force (FATF) highlighted the use of decentralized exchanges (DEXs) and cross-chain bridges as key tools for money launderers. Elliptic's Topology report 2024 touch upon the emerging use of stable coins, crypto ATMs, peeling – chain, sanction evasion and artificial intelligence enabling criminals to scale their frauds.

Case Studies Highlighting Cryptocurrency's Role in Money Laundering

Several high-profile cases have illustrated the challenges of regulating cryptocurrency-based money laundering. For example, on March 23, 2022, the Lazarus Group, a DPRK state-sponsored cyber hacking group, carried out the largest virtual assets heist to date, worth almost $620 million, from a blockchain project linked to the online game Axie Infinity. They also stole $100 million worth of virtual assets from a cross-chain bridge called Horizon.

Another notable example is 'Korvio Coin', promoted as lucrative investment opportunity promising substantial returns that duped ₹2,500 Crore affected approximately 2.5 lakh individuals.

Continuing further, in 2022 U.S. authorities seized more than $3.6 billion in allegedly stolen bitcoins linked to the 2016 hack of Bitfinex. The hackers used mixers and anonymous wallets to launder the stolen Bitcoin over several years, showcasing the sophisticated techniques criminals use in the crypto space.

In February 2024, Homeland Security Investigations (HSI) charged Rhoden and Nowlin for NFT money laundering. They orchestrated NFT collections on the Solana blockchain, culminating in a "rug pull" that defrauded investors of approximately $135,000. They used chain-hopping to obscure the illicit funds, converting them into U.S. dollars and bank deposits, totalling over $300,000.

One of India's largest crypto exchange WazirX had a $230 million hack in July 2024 resulting in a loss of nearly 45% of its holding assets. According to Elliptic's analysis the breach was made up of more than 200 different assets and the hacker has swapped those using a variety of decentralised services, a typical step of laundering process.

These examples illustrate only a fraction of the extensive and complex landscape of cryptocurrency-related money laundering. This reveals critical gaps in current regulatory framework, which struggles to keep pace with the evolving methods of illicit actors.

Regulatory Responses and Challenges

The G20's adoption of the FATF 2019 standards for virtual asset service providers was a significant step toward mitigating these risks, yet implementation remains uneven across jurisdictions. According to a FATF Survey, as of April 2023, 35 out of 135 responding jurisdictions reported having passed "Travel Rule", which mandates the sharing of customer information during cryptocurrency transactions, while 27 jurisdictions have begun implementing enforcement and supervisory measures. The European Union has initiated regulatory measures with the implementation of the 5th Anti-Money Laundering Directive (5AMLD), marking the beginning of a more comprehensive framework for regulating virtual currencies. It has also provided recommendations for public and private sector stakeholders across the EU.

The lack of uniformity in global regulations allows criminals to exploit jurisdictions with lax enforcement. Moreover, privacy coins such as Monero and ZCash, which obscure transaction details, present additional challenges for regulators. A 2023 study by Bruegel, highlighted the difficulty in tracking these coins, which are increasingly favoured by criminals for their enhanced privacy features.

By combining theoretical insights with practical investigations, this research aims to bridge the gaps identified in the regulatory responses and to address these challenges, it is crucial to build on existing research with practical studies.

Tracking cryptocurrency transaction

Many believe the cryptocurrency transactions are anonyms but in an open blockchain network, every transaction and the wallets involved are transparently recorded in the ledger using cryptographic hashes. Not only the transaction hash but the hash values of wallets and transactions associated with those wallets is publicly available. As can be seen from the figures below, we have considered a transaction from Bitcoin Block 132,998 having hash 1Le7x23sdhRM1YLaLy5kGTUf7ecb1D5uXZ of 6633.928 BTC which is associated with wallet address 1Le7x-D5uXZ (Figure 2). We examined the transactions from blockchain.com (Figure 2) and btcscan.org (Figure 3) both contains same information for the same transaction (hash). This confirms the value of transaction and the accounts in which it took place.

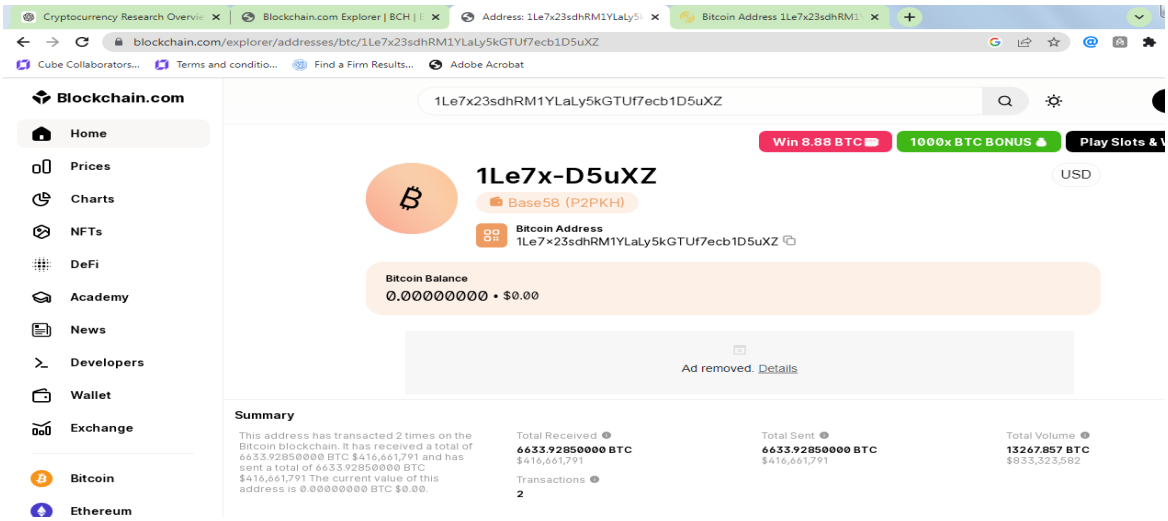

Figure 2: Screenshot from Blockchain.com

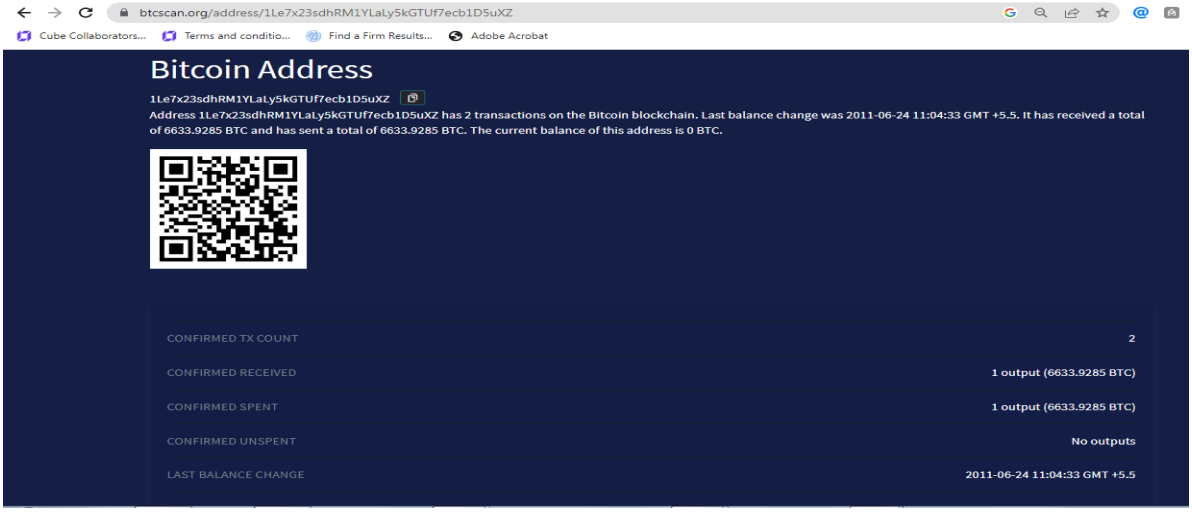

Figure 3: Screenshot from Btcscan.org

Moving further, we used digital forensic tool "Blockchaintracer" to trace the trail of bitcoin transaction in this wallet. Bitcoin payments are forward tracked so that, given a set of starting nodes, a search is conducted for patterns of coin transfer to other entities in split sums. Here, the Red circle is the wallet (Figure 4) which gives the total incoming and outgoing transactions in this wallet. The Pink circle (Figure 5) denotes the wallet from which the incoming to the wallet happened. As can be shown as the arrow rightly pointed to Red. Following which there are 2 circles, Orange and Grey (Figure 6 & 7) which reflect the wallet address of the recipient of Bitcoins from our wallet. This gives the transactional graph of the wallet in question. Clicking Orange further, we get the details of the transactions in that wallet providing trail of fund flow (Figure 8).

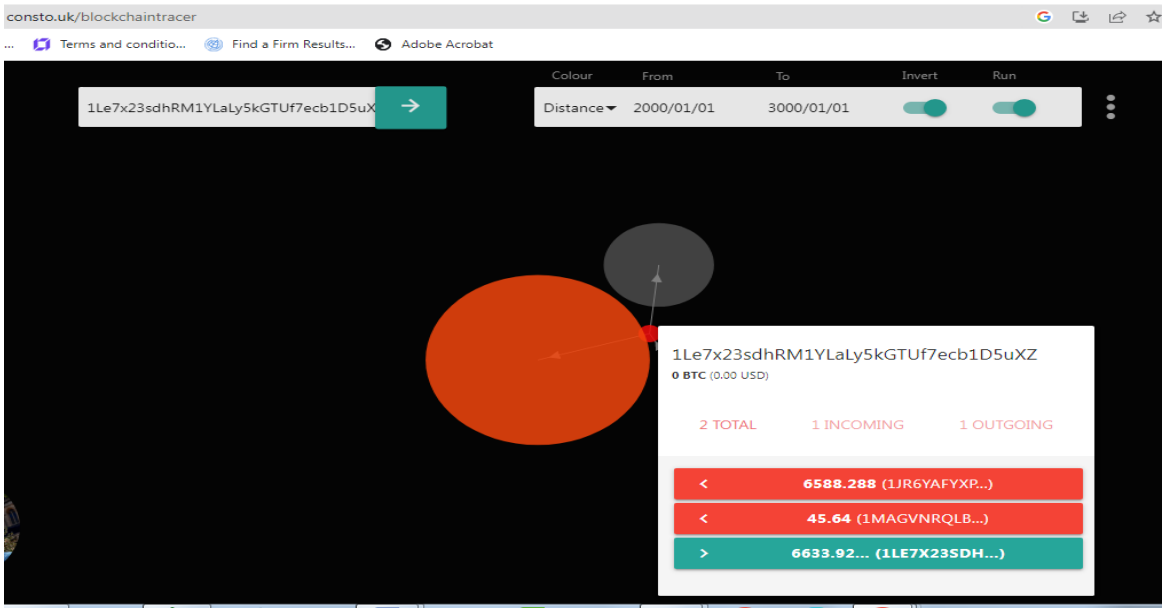

Figure 4: Transactions details of the hash investigated - 1Le7x23sdhRM1YLaLy5kGTUf7ecb1D5uXZ

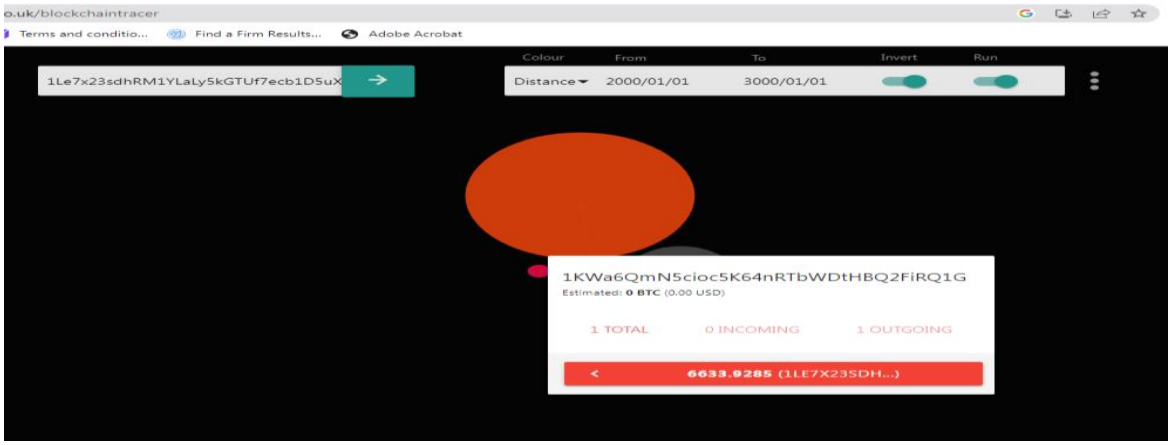

Figure 5: Wallet from which Bitcoins were transferred to our wallet

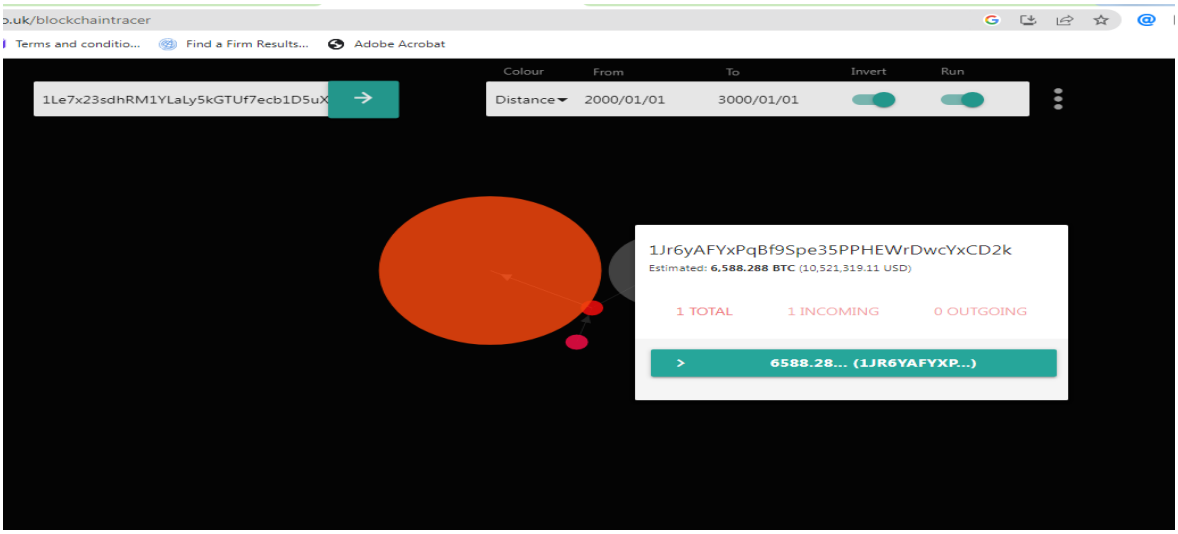

Figure 6: Wallet to which Bitcoins were transferred from our wallet

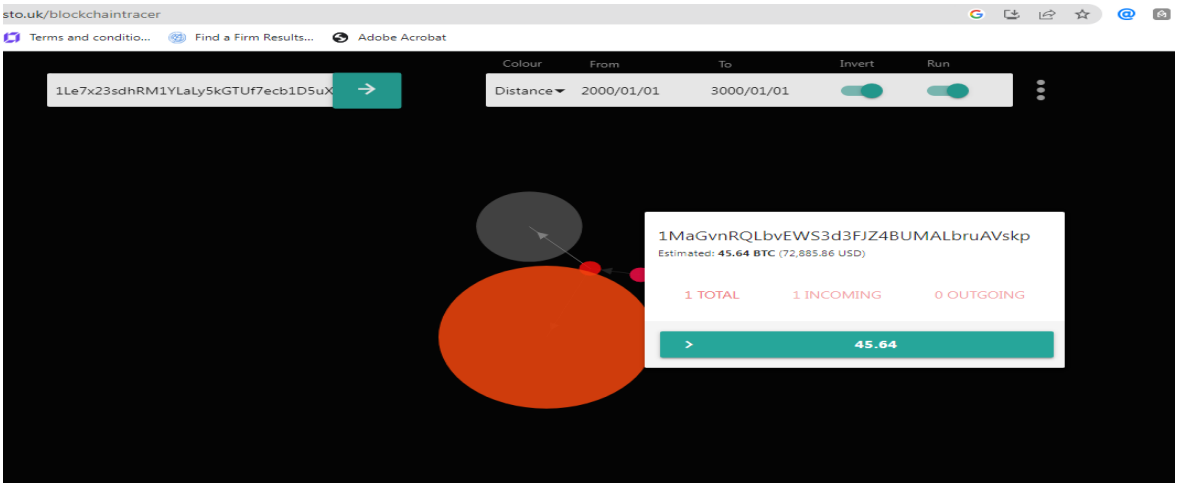

Figure 7: Wallet to which Bitcoins were transferred from our wallet

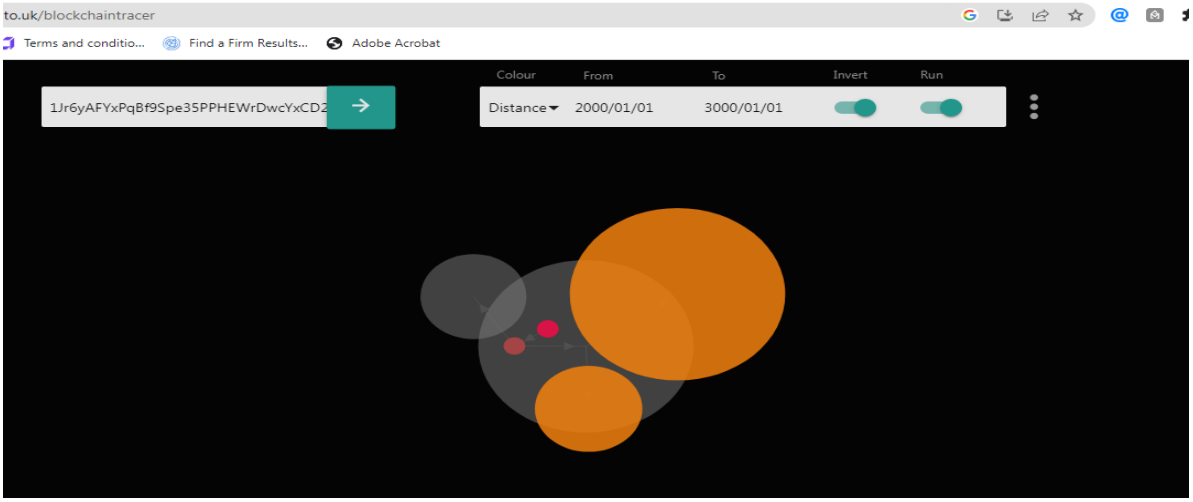

Figure 8: Transactions of the wallet in which base wallet have transferred Bitcoins

Tracking transactions processed through coin mixers

One of the most deceiving tools used by launderers to obfuscate the flow of funds is Mixers. Instead of simply sending coins to desired addresses they utilize coin mixers to transfer funds across multiple accounts, at multiple timelines and in differential proportions making it extremely challenging to trace the origin and destination.

We have examined a specific transaction with the hash 'd439c2bd8b164fd555d43d0fad903b7f06c4739855d55f87e452be1f6fb47578' to trace its path and determine whether coin mixers were involved. It is observed, this transaction has 128 inputs but only 2 outputs which seem to be the collection of money at various addresses belonging to the mixing service followed by a transfer to two distinct addresses via a sweeper transaction identifying a potential initial transaction. (Figure 9)

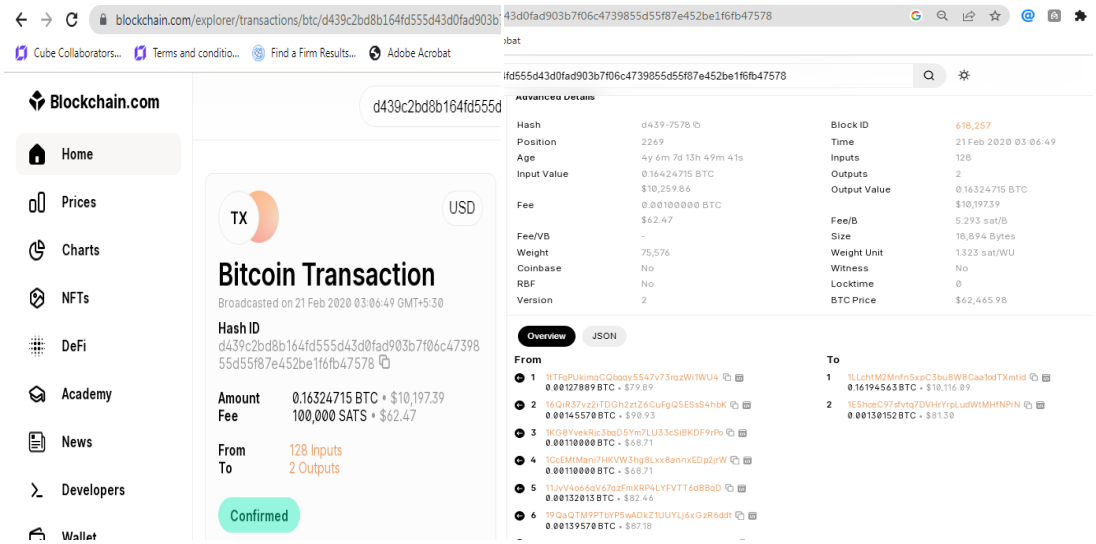

Figure 9: Tracing of hash for tracking transactions processed through coin mixers

From this transaction, we have constructed forward transaction flow using Blockchaintracer. By analyzing the two outputs, we observed a similar transaction pattern involving multiple inputs

(highlighted in red) and fewer outputs (highlighted in orange). This pattern indicates the use of mixing techniques, where funds are dispersed through several transactions before reaching their final destination. Figures 10 and 11 illustrate this mixing pattern and its impact on the movement of illicit funds.

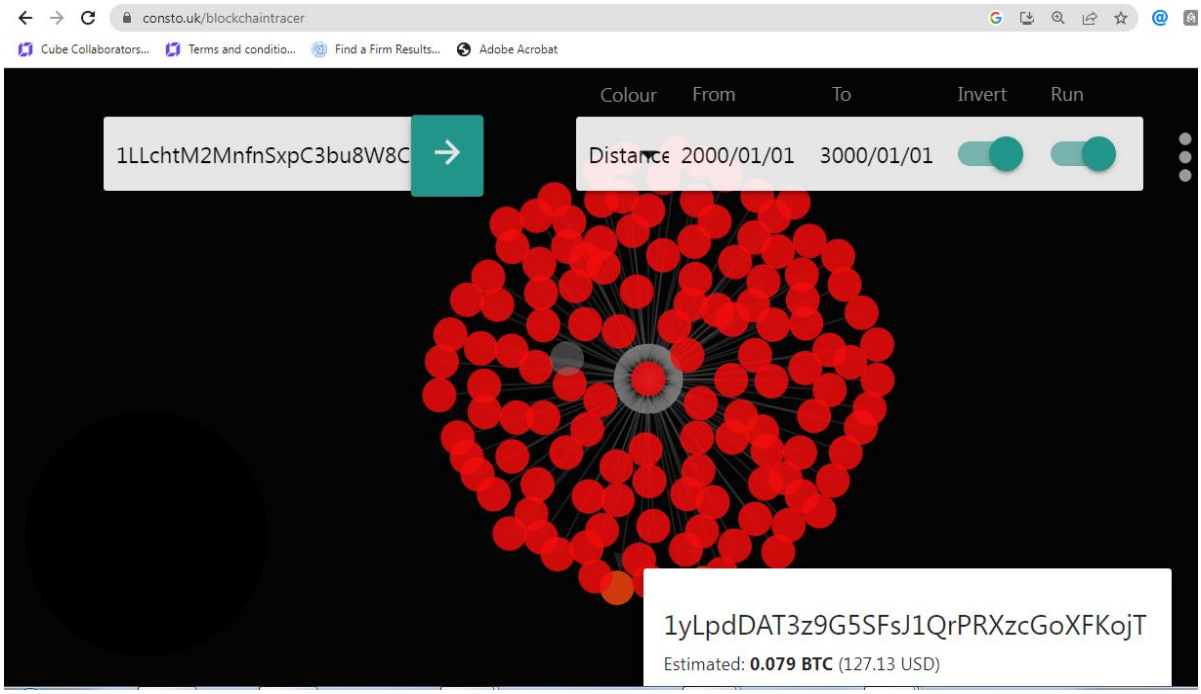

Figure 10: Detailed transaction flow in the preliminary output 1 wallet having hash 1LLchtM2MnfnSxpC3bu8W8Caa1odTXmtid.

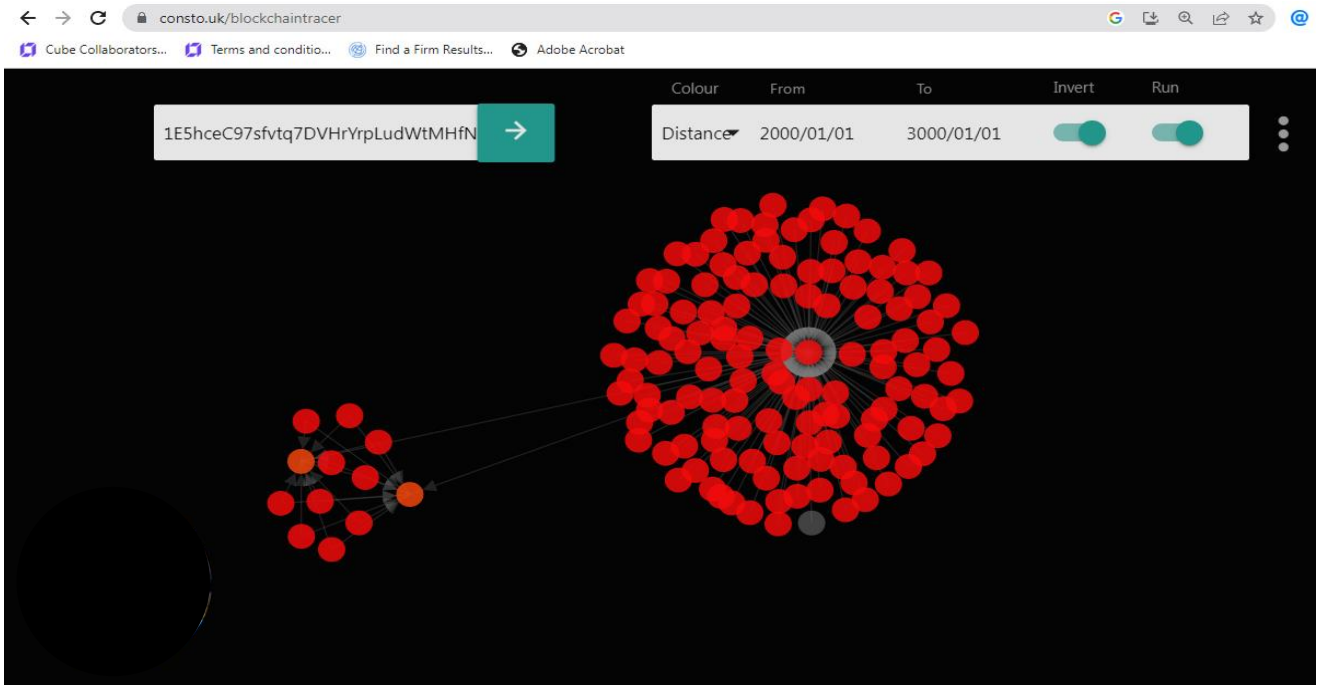

Figure 11: Detailed transaction flow in the preliminary output 2 wallet having hash 1E5hceC97sfvtq7DVHrYrpLudWtMHfNPrN.

Expanding the transaction trail to its full extent, until reaching either the final destination or an anomaly exceeding the established threshold, provides a comprehensive overview of the destination wallets where the cryptocurrency ultimately lands (Figure 12). This analysis provides valuable insights into the use of mixers in manipulating fund flow.

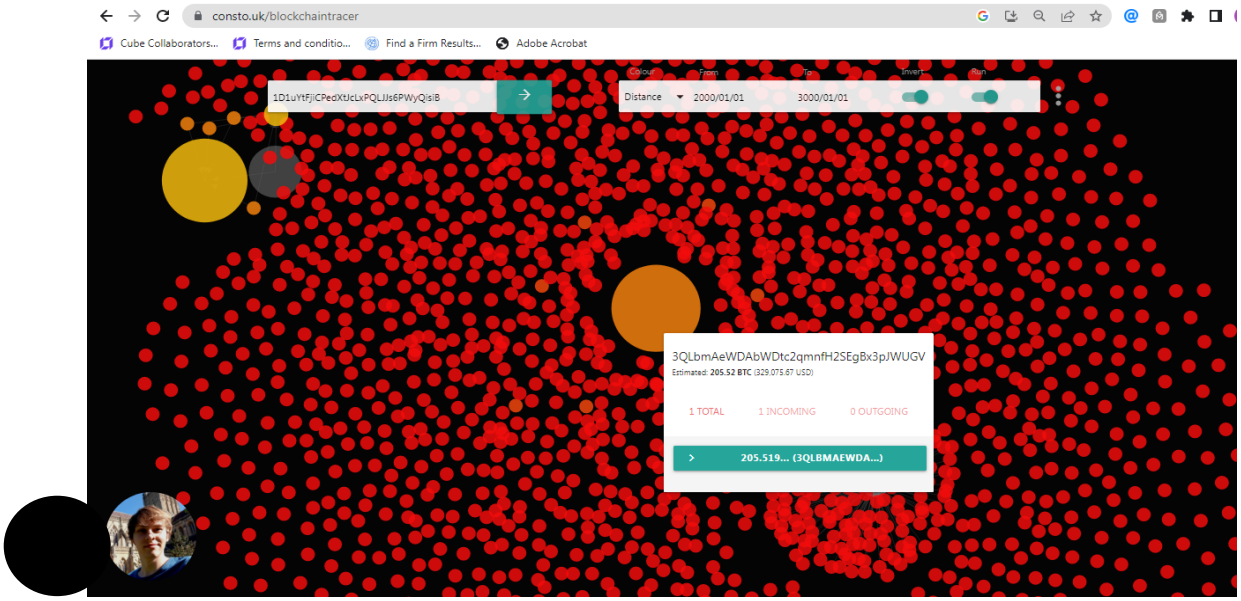

Figure 12: Bird's eye view of transaction trail.

4. Analysis

Our research substantiates the argument that true anonymity in open blockchain systems is a myth. Through meticulous tracing of blockchain transactions, we demonstrated that even complex transactions involving coin mixers can be traced back to their origins, undermining claims of complete anonymity. In our study we identified patterns indicative of coin mixer usage. The analysed transaction was indicative of a mixing pattern where funds were consolidated at mixer addresses before being distributed to final destinations.

Our analysis confirms that while mixers obscure the direct trail of funds, they do not render transactions completely untraceable. By expanding the transaction trail, we were able to uncover the movement of funds and reveal the endpoints of these transactions. This aligns with findings from Elliptic's Topology report and other referenced studies, which highlight the challenges and limits of mixers in ensuring true financial anonymity. The proposed solutions presented in this study are applicable on low volume transactions and straightforward operational logic, the analysis becomes more complex in decentralised, voluminous and privacy transactions making it difficult to trace the illicit transaction to its origin or destination.

Though, more sophisticated digital forensic tools, advancements in learning algorithms, heuristic methods, cross chain tracking, compliance checks and collaboration between authorities can significantly improve the ability to trace and analyze cryptocurrency transactions. The disparities in regulatory responses, such as those highlighted in the FATF standards and the EU's 5AMLD, further complicate the landscape. Despite advancements in regulation, our findings emphasize that gaps remain, particularly in addressing privacy coins and the effectiveness of enforcement. The variability in global regulatory practices provides loopholes that can be exploited by sophisticated laundering schemes. Our

practical analysis builds upon these insights, demonstrating that while regulatory frameworks are developing, they must evolve alongside forensic techniques to address emerging challenges effectively.

5. Conclusion

We are living in the era of unprecedented technological evolution where innovations like blockchain, decentralized finance (DeFi), artificial intelligence, quantum computing, robotics are transforming the world. In this rapidly changing landscape, our research has focused on one critical aspect: the role of cryptocurrencies in financial systems. The increasing popularity of digital currencies underscores the rapidly expanding potential of the cryptocurrency landscape. As with any groundbreaking technology, cryptocurrencies bring forth a duality of promise and peril. While they offer unprecedented ease and efficiency in global financial transactions, they also present significant challenges, particularly in the realm of anonymity and illicit activities.

Cryptocurrencies have emerged as powerful financial tools for criminal and terrorist networks, exploiting their decentralized nature, peer-to-peer systems, and the promise of anonymity. Within our borderless digital world, the issue of illegal finances transcends national boundaries and navigates through varied jurisdictional landscapes. The intricate nature of the digital economy, coupled with rapidly advancing technologies, allows money to be illicitly earned and transferred across borders with just a click. Yet, these illicit operations are not beyond the reach of modern forensic methods. While criminals increasingly utilize advanced methods to conceal their activities, law enforcement agencies and governments are equally committed to unmasking them.

Our study highlights the intricate dynamics of cryptocurrency-related financial crimes, shedding light on the real-life case studies and evolving tactics employed by criminals, such as the use of NFTs, coin mixers and complex transaction patterns to obscure illicit activities. Anonymity is something criminals rely upon, but data on the blockchain is transparent in terms of transaction details but anonyms in terms of identity details. As we identified we can get to the origin and destination wallet address, which alone do not reveal any identifiable details. However, the identity can be traced through the IP addresses used, timestamp scrutinies, social engineering techniques, cross referencing with data leaks, digital forensic tools, use of artificial intelligence, deep learning techniques, increased collaborations and data sharing between regulatory bodies and law enforcement agencies.

Furthermore, strengthening and harmonizing global recommendations and regulations across jurisdictions will create a more unified approach to oversight, reducing opportunities for regulatory evasion and ensuring that all cryptocurrency activities are subject to rigorous scrutiny. Encouraging cryptocurrency exchanges and financial institutions to adopt robust anti-money laundering (AML) and counter-terrorist financing (CTF) compliance measures is crucial. This includes performing thorough Know Your Customer (KYC) checks, regular audits, monitoring transactions for suspicious activities, and reporting such activities to the relevant authorities.

The future is approaching swiftly, bringing transformative technologies that will redefine our world. As we look ahead, it is crucial to remain vigilant and adaptive, continually refining our strategies to keep pace with the rapid evolution of digital finance. This research reflects commitment to understanding and mitigating the money laundering risks associated with cryptocurrencies, contributing to a more secure and transparent financial ecosystem as we embrace the transformative changes ahead.

7. References

1. 2 charged with NFT money laundering, 'Rug pull' of digital blockchains | Homeland security. (2024, February 23). U.S. Department of Homeland Security. https://www.dhs.gov/hsi/news/2024/02/23/2-charged-nft-money-laundering-rug-pull-digital-blockchains
2. Angert, A., Deininger, S., Lyons, K., Sec+, CFE, Kachenko, C., Saint Cyr, D. E., CPA, CFE, CCI, Peters, K., Wahlgren, M., CFCS, Malarkey, M., Novak, K., Federal Bureau of Investigation, National Security Agency, U.S. Secret Service, Federal Reserve Bank of Cleveland, U.S. Department of Defense, Western Union, Invesco, & National Insurance Crime Bureau. (n.d.). Private and public sector analysis of illicit finance activities in the cyber financial landscape. https://www.dhs.gov/sites/default/files/2022-09/Combatting%20Illicit%20Activity%20.pdf
3. Bååth, D., & Zellhorn, F. (2016). How to combat money laundering in Bitcoin? An institutional and game theoretic approach to anti-money laundering prevention measures aimed at Bitcoin. In Göran Hägg & Peter Andersson, Masteruppsats i Nationalekonomi Internationella Civilekonomprogrammet. https://www.diva-portal.org/smash/get/diva2:1039181/FULLTEXT01.pdf
4. Banamex USA Agrees to Forfeit $97 Million in Connection with Bank Secrecy Act Violations. (2024). https://www.justice.gov/opa/pr/banamex-usa-agrees-forfeit-97-million-connection-bank-secrecy-act-violations
5. Bank sentenced for obstructing regulators, forfeits $368 million for concealing Anti-Money laundering failures. (2024, July 8). https://www.justice.gov/usao-sdca/pr/bank-sentenced-obstructing-regulators-forfeits-368-million-concealing-anti-money
6. Barone, R., & Masciandaro, D. (2019). Cryptocurrency or usury? Crime and alternative money laundering techniques. European Journal of Law and Economics, 47(2), 233–254. https://doi.org/10.1007/s10657-019-09609-6
7. Benson, V., Turksen, U., & Adamyk, B. (2023). Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities. Journal of Financial Regulation and Compliance, 32(1), 80–97. https://doi.org/10.1108/jfrc-04-2023-0065
8. Bitfinex hacker and wife plead guilty to money laundering conspiracy involving billions in cryptocurrency. (2023). https://www.justice.gov/opa/pr/bitfinex-hacker-and-wife-plead-guilty-money-laundering-conspiracy-involving-billions#:~:text=Ilya%20Lichtenstein%2C%2035%2C%20and%20Heather,valued%20at%20approximately%20%243.6%20billion.
9. Blockopedia. (2023, November 7). The Blockopedia(@The_Blockopedia)'s insights [Online forum post]. Binance Square. https://www.binance.com/en-IN/square/post/1667087
10. Coffman, D. (2024). The ascent of money: a financial history of the world. By Niall Ferguson. London: Allen Lane, 2008. Pp. 442. ISBN 978-1-846-14106-5
11. Crackdown on money mule service providers laundering over EUR 10 million | Europol. (n.d.-a). Europol. https://www.europol.europa.eu/media-press/newsroom/news/crackdown-money-mule-service-providers-laundering-over-eur-10-million
12. Cryptocurrency frauds. (2020). In International Journal of Engineering and Advanced Technology (IJEAT) (pp. 261–262). Blue Eyes Intelligence Engineering and Sciences Publication. https://doi.org/10.35940/ijeat.F1391.089620
13. Desk, T. T. (2024, January 21). RBI governor Shaktikanta Das has two-word warning for cryptocurrency investors in India. https://timesofindia.indiatimes.com/gadgets-news/rbi-governor-

shaktikanta-das-warns-indian-cryptocurrency-investors/articleshow/106925220.cms
14. Dupuis, D., & Gleason, K. (2020). Money laundering with cryptocurrency: open doors and the regulatory dialectic. Journal of Financial Crime, 28(1), 60–74. https://doi.org/10.1108/jfc-06-2020-0113
15. Elliptic. (2020). Financial Crime Typologies in Cryptoassets: The Concise Guide for Compliance Leaders. https://www.elliptic.co/hubfs/Financial%20Crime%20Typologies%20in%20Cryptoassets%20Guides%20(All%20Assets)/Typologies_Concise%20Guide_12-20.pdf
16. Elliptic. (2023). The State of Cross-chain Crime Report 2023 | Elliptic. The State of Cross-chain Crime 2023. https://www.elliptic.co/resources/state-of-cross-chain-crime-2023
17. Elliptic. (2024). Typologies Report 2023 | Elliptic. Elliptic. https://www.elliptic.co/resources/elliptic-typologies-report-2023
18. Elliptic. (2024). Typologies Report 2024 | Elliptic. Typologies Report 2024. https://www.elliptic.co/resources/elliptic-typologies-report-2024
19. European Union Agency for Law Enforcement Cooperation. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. In Publications Office of the European Union [Report]. Publications Office of the European Union. https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202024%20-%20EN_0.pdf
20. Financial Action Task Force. (2022). Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPS. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf
21. Financial Crime Academy. (2024, August 22). Understanding crypto money laundering methods: The Cryptocurrency Crime. Financial Crime Academy. https://financialcrimeacademy.org/cryptocurrency-money-laundering-methods/
22. Financial Intelligence Centre (FIC). (2023). What is a money mule?https://www.fic.gov.za/wp-content/uploads/2024/06/Financial-Crime-Insights-Money-mules.pdf
23. FIU-India. (n.d.). https://fiuindia.gov.in/files/AML_Legislation/pmla_2002.html
24. Greig, J. (2022, January 26). Report: Cybercriminals laundered at least $8.6 billion worth of cryptocurrency in 2021. ZDNET. https://www.zdnet.com/finance/blockchain/cybercriminals-laundered-at-least-8-6-billion-worth-of-cryptocurrency-in-2021/
25. Han, J., Huang, Y., Liu, S., & Towey, K. (2020). Artificial intelligence for anti-money laundering: a review and extension. Digital Finance, 2(3–4), 211–239. https://doi.org/10.1007/s42521-020-00023-1
26. Keatinge, T., Carlisle, D., Keen, F., Directorate General for Internal Policies, & Policy Department for Citizens' Rights and Constitutional Affairs. (2018). Virtual currencies and terrorist financing: assessing the risks and evaluating responses [Study]. In Policy Department for Citizens' Rights and Constitutional Affairs (pp. 3–85). https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf
27. Lazarus Group hackers appear to return to Tornado Cash for money laundering. (n.d.). https://therecord.media/lazarus-group-north-korea-tornado-cash-money-

laundering#:~:text=According%20to%20the%20Treasury%20Department,%24100%20million%20taken%20from%20Horizon
28. Lebanese businessman tied by Treasury Department to Hezbollah pleads guilty to money laundering conspiracy in furtherance of violations of U.S. sanctions. (2024, May 30). https://www.justice.gov/opa/pr/lebanese-businessman-tied-treasury-department-hezbollah-pleads-guilty-money-laundering
29. Moreno-Sanchez, P., Ruffing, T., & Kate, A. (2021). PathShuffle: Credit mixing and anonymous payments for Ripple. In Proceedings on Privacy Enhancing Technologies (pp. 1–20) [Journal-article]. https://www.cs.purdue.edu/homes/akate/publications/PathShuffle.pdf
30. Nakamoto, S. (n.d.). Bitcoin: a Peer-to-Peer electronic cash system. https://bitcoin.org/bitcoin.pdf
31. Paesano, F. (n.d.). Cryptocurrencies and money laundering investigations. https://baselgovernance.org/sites/default/files/2023-08/230822_quick_guide_update_en.pdf
32. Pakki, J., Shoshitaishvili, Y., Wang, R., Bao, T., Doup´E, A., & Arizona State University. (2021). Everything You Ever Wanted to Know About Bitcoin Mixers (But Were Afraid to Ask). Arizona State University. https://yancomm.net/papers/2021%20-%20Financial%20Crypto%20-%20Bitcoin%20Mixers.pdf
33. Shojaeinasab, A., Motamed, A. P., & Bahrak, B. (2023). Mixing detection on Bitcoin transactions using statistical patterns. IET Blockchain, 3(3), 136–148. https://doi.org/10.1049/blc2.12036
34. Stokes, R. (2012). Virtual money laundering: the case of Bitcoin and the Linden dollar. Information & Communications Technology Law, 21(3), 221–236. https://doi.org/10.1080/13600834.2012.744225
35. Team, C. (2020, January 15). Crypto money laundering: How criminals cash out billions in Bitcoin and other cryptocurrencies. Chainalysis. https://www.chainalysis.com/blog/crypto-laundering/#:~:text=While%20it's%20difficult%20to%20estimate,hide%20the%20nature%20of%20their
36. Team, C. (2022, August 23). Crypto mixers and AML compliance. Chainalysis. https://www.chainalysis.com/blog/crypto-mixers/
37. The Chainalysis 2024 Crypto Crime Report. (n.d.). https://go.chainalysis.com/crypto-crime-2024.html
38. The Monero Project. (n.d.). getmonero.org, the Monero Project. https://www.getmonero.org/
39. Tsuchiya, Y., & Hiramoto, N. (2021). How cryptocurrency is laundered: Case study of Coincheck hacking incident. Forensic Science International Reports, 4, 100241. https://doi.org/10.1016/j.fsir.2021.100241
40. Two Chinese Nationals Charged with Laundering Over "00 Million in Cryptocurrency From Exchange Hack. (2022, July 22). https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack
41. U. S. Department of The Treasury. (2023). Illicit Finance Risk assessment of decentralized finance. https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf
42. UNODC. (2022). Financial investigations of money laundering involving Virtual Assets. https://www.unodc.org/documents/commissions/CND/Subsidiary_Bodies/HONEUR/15_HONEUR_2023/6b_VA_FinInvestigations_GPML_AB1_for_Alexandra_22_June.pdf
43. Western Union Admits Anti-Money Laundering and Consumer Fraud Violations, Forfeits $586 Million in Settlement with Justice Department and Federal Trade Commission. (2024, May 30).

https://www.justice.gov/opa/pr/western-union-admits-anti-money-laundering-and-consumer-fraud-violations-forfeits-586-million

44. Zhang, Y., Yang, D., & Colorado School of Mines. (2019). RobustPay: Robust Payment Routing Protocol in Blockchain-based Payment Channel Networks. IEEE 27th International Conference on Network Protocols (ICNP)