

*The Use of Crypto Assets in Money Laundering and the Measures to Be Taken Against It ***

*Prof. Dr. Murat Volkan Dölger***

Abstract

With the advancement of technology day by day, there are many positive and negative developments in the field of law as in many other fields. In the field of criminal law, sometimes new types of offences occur, and sometimes the way in which existing types of offences are committed changes. In recent years, with the inclusion of crypto assets in our lives, the crime of money laundering by using crypto assets is frequently on the agenda. In this study, it is explained whether crypto assets are used for laundering the proceeds of crime, the methods by which crypto assets are used to commit crimes, what are the risks arising for this reason and what kind of measures should be taken against this. Finally, the legal arrangements made in Türkiye are included

Key Words: crypto asset, crypto money, money laundering, proceeds of crime, laundering of proceeds of crime, blockchain, distributed ledger technology.

Introduction

The use of crypto assets for laundering the proceeds of crime, or as it is commonly known by the public, money laundering, is increasingly becoming a topic of discussion. It is influenced by the frequent inclusion of this phenomenon in academic literature as well as in the work and regulations of national and international organizations combating money laundering. Another important factor in this context is the significant role that crypto assets have recently played in investigations related to money laundering in Türkiye.¹ Simultaneously across various parts of Türkiye,

** This article is the translated version of the article published in Istanbul Aydın University Faculty of Law Journal, Vol. 10, No. 1, 2024, pp. 41-94, carried out by the author using ChatGPT-4 Plus. The translation has been edited by the author, who assumes full responsibility for its accuracy.

** Professor of the Department of Criminal Law and Criminal Procedure Law at Istanbul Aydın University Faculty of Law. <https://orcid.org/0000-0003-4034-5436>

¹ Indeed, due to these investigations demonstrating the seriousness of combating money laundering in Türkiye, which had been on the FATF's grey list for three years, was removed from the list as of June 2024. Another important step in this regard was the introduction of regulations concerning crypto assets in the Capital Markets Law. For detailed information on the process of Turkey's inclusion in this list and the reasons for it, see. **Hüseyin Işık**, "Mali Eylem Görev Gücü'nün (FATF) Gri Listesi ve Türkiye", International Journal of Public Finance, Vol. 7, No. 2, 2022, p. 414-421.

"Countries that fail to comply with recommendations are included in the blacklist, while those that partially comply are included in the grey list. Countries that implement FATF recommendations to a significant extent are not included in any list. Being listed indicates that the relevant country has certain vulnerabilities regarding

investigations and prosecutions are being conducted for crimes such as laundering proceeds of crime (Article 282 of the Turkish Penal Code, TPC), providing a place and opportunity for gambling (Article 181, TPC), illegal acquisition (Article 135, TPC) and transfer of personal data (Article 136, TPC), and establishing or joining an organization to commit crimes (Article 220, TPC). Many suspects are detained during these investigations, a significant portion of whom are arrested and remain in custody for quite long periods.

At the international level, organizations combating money laundering and terrorist financing, as well as other international bodies, have expressed opinions and adopted risk-based approaches regarding the use of crypto assets in laundering and financing terrorism. However, the extent to which these approaches and the perceptions created reflect reality is debatable. Nevertheless, money laundering through crypto assets is becoming an increasingly significant concern for governments and law enforcement agencies worldwide.²

A great deal can be written about crypto assets, their characteristics, and how regulations regarding these assets should be structured. However, the focus of this article lies in the intersection of crypto assets and the laundering of proceeds of crime. Nevertheless, this intersection is quite broad due to the multifaceted nature of both topics. Therefore, we can narrow down the main topics we wish to discuss in this article with the following questions and outline the boundaries of our study.

In this context, is merely holding, buying, selling, or conducting an initial public offering of crypto assets a crime? Do these transactions have any aspect that violates the law? Leaving other crimes aside, are crypto assets truly used for laundering proceeds of crime as much as claimed? Do these tools genuinely facilitate and increase money laundering activities? Is the association of these tools with money laundering a current problem, or is it a precaution for the future? In the investigations carried out in Türkiye on this subject, are these tools genuinely being targeted, or is there another purpose? What kind of regulation has been implemented in Türkiye regarding this issue? In this study, we aim to answer all these questions.

FATF recommendations. The announcement of the FATF list generates significant reactions both in the global public opinion and domestically. Türkiye underwent a mutual evaluation in 2019. Following this evaluation, a report was published in December of the same year. After the publication of this report, it was expected that Türkiye would address the issues highlighted in the criticisms. However, as it was stated that no progress was made on the criticized points, Türkiye was placed on the Grey List during the FATF General Assembly meeting in October 2021. The inclusion in the Grey List also sparked significant debate in the domestic public sphere." (Işık, p. 408)

² Romel Sharif, "Digital Bill: An Approach to Minimize Illicit Activities and other Drawbacks of Crypto Currency", May 2023, (Online) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4434303, (Accessed 28.07.2024).

Definition and Emergence of Crypto Assets

Before discussing how crypto assets can be used to facilitate the laundering of proceeds of crime, it is essential to understand what a crypto asset is.

A crypto asset can be defined as “a unit of digital asset that exists solely in digital form, typically without a centralized issuer or regulatory authority, instead using a decentralized system to record transactions.” Unlike fiat (traditional)³ currencies, crypto assets are not issued by any central authority, nor are they backed by any state guarantee. This means there is “no protection for the buyer or seller, and their use as payment is entirely voluntary.”⁴

Therefore, these assets, built on blockchain technology, do not have a centralized structure due to the inherent nature of the technology on which they are based.⁵ This also results in the absence of a centralized record during transactions and the emergence of a semi-anonymous structure. This semi-anonymous nature and decentralization, on the one hand, attract criminals who wish to avoid detection, while on the other hand, make the work of judicial authorities more difficult. Additionally, the ability to create unlimited accounts to an extent that makes it impossible to monitor transactions, the possibility of person-to-person transfers through crypto asset intermediaries (exchanges), and the ability to conceal financial activities are other factors that make crypto assets a preferred tool for laundering proceeds of crime.⁶

Among crypto assets, the oldest, most well-known, and most widely used is Bitcoin, which was first introduced in 2008 by Satoshi Nakamoto.⁷ However, it is believed that this name is a pseudonym. Since Bitcoin’s introduction, there has been significant speculation regarding the real identity or identities of its developer(s), but Satoshi’s identity remains an unsolved mystery. Bitcoin was introduced to the world following the 2008 financial crisis with the aim of serving as an alternative currency free from corporate interventions and government regulations. Individuals who own Bitcoin can use it freely without restrictions and move their funds worldwide without the need for

³ Fiat, or in other words, traditional currency, refers to money issued based on government decisions, not backed by gold, silver, or similar reserves. It is built on trust in the issuing authority and the non-replicability of the paper on which it is printed. Fiat currency is used for the exchange of goods and services and typically exists as banknotes or paper money. The currencies currently in circulation today follow this structure.

⁴ **George Forgang**, Money Laundering Through Cryptocurrencies, Unpublished Master of Science Thesis, La Salle University Economic Crime Forensics Capstones 40, 2019, s. 4 (Online) https://digitalcommons.lasalle.edu/ecf_capstones/40, (set) 15.06.2024.

⁵ **Kerim Çakır**, Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu, 2. Edition, Adalet Yayınevi, Ankara, 2023, p. 77.

⁶ **Murat Balcı/Kerim Çakır**, Kripto Paraların Karapara Aklama Yöntemi Olarak Kullanılması, CHD, Year: 16, Issue: 46, August, 2021, p. 317.

⁷ **Satoshi Nakamoto**, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 30th October 2008, (Online) <https://bitcoin.org/bitcoin.pdf>, (Accessed 11.07.2024); **Çakır**, p. 77; **Berrin Akbulut**, “Kripto Para ve Terörizmin Finansmanı”, Karşılaştırmalı Hukukta ve Türk Hukukunda Terörizm, Terör Suçları ve İnfaz Hukuku, Ed. İzzet Özgenç, Volume 1, Türkiye Bilimler Akademisi, Ankara, 2024, p. 487.

a financial intermediary. According to a popular anecdote, a man in Florida once offered 10,000 Bitcoin in exchange for pizza (at the time, Bitcoin was worth far less than it is today). A person in the United Kingdom accepted the offer and arranged for two Papa John's pizzas to be delivered to the Bitcoin user in Florida.⁸ If the story is true, these pizzas are likely the most expensive pizzas ever sold to date. This transaction is known as the first recorded use of Bitcoin. While this transaction was harmless and mundane on its own, Bitcoin's anonymity feature and lack of regulation quickly caught the attention of criminals, leading to its misuse for malicious purposes in a short period.⁹ The widespread association of Bitcoin, and consequently crypto assets, with crime, and the perception that it is merely a tool for committing crimes, is primarily due to the online marketplace "Silk Road", which operated between 2011 and 2013. Initially, Silk Road served as an anonymous and secure marketplace for its users but later became a platform exploited by malicious actors for drug trafficking and money laundering (black money).¹⁰ This site operated on the "dark net" allowing individuals with access to the site to buy and sell a wide range of illegal goods without the threat of being caught. While the site was active, it is estimated that over 100,000 users conducted transactions worth more than \$200 million in illegal goods, including drugs, fake IDs, and pornography.¹¹ Following an extensive investigation, the website was shut down by the FBI, and its administrator, Ross Ulbricht, was arrested on charges of money laundering and drug trafficking. Additionally, the U.S. Department of Justice seized approximately \$3.5 to \$4 million worth of Bitcoin.¹²

The unauthorized possession, transfer, purchase, and sale of products such as drugs or weapons, which are prohibited, being conducted online without any legal regulation is a significant problem on its own. In addition, the Silk Road incident demonstrated to authorities that Bitcoin could be used to facilitate such illegal activities and, therefore, should not be perceived merely as an innocent innovation.¹³ While Silk Road was operational, Bitcoin was the only crypto asset in circulation. Since then, thousands of new crypto asset units have been introduced to the market. Technically, all cryptocurrencies that are not Bitcoin are considered "altcoins." Among these, *Ethereum* and *Ripple* are the two crypto assets with the highest value after Bitcoin, which seemingly makes them the most recognized, transferable, and, though

⁸ **Alison Griswold**, "The First-Ever Bitcoin Purchase Was Remarkably Inglorious" *Slate*, 23.05.2014, <https://slate.com/business/2014/05/first-bitcoin-purchase-two-pepperoni-pizzas-from-papajohn-s.html>

⁹ **Forgang**, p. 4, 5. For specific cases of Bitcoin misuse, see. **Sesha Kethineni/Ying Cao/Cassandra Dodge**, "Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes," *American Journal of Criminal Justice*, Vol. 43, Issue 2, May 2017.

¹⁰ **Balcı/Çakır**, p. 323

¹¹ **Corinne Ramey**, "The Crypto Crime Wave is Here" *The Wall Street Journal*, April 26 2018, (Online) <https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366>, (Accessed 10.07.2024).

¹² **Arnold Greenberg**, (2018, April 23). "The Dark Web's Favorite Currency Is Less Untraceable Than It Seems", *Wired* (Online) <https://www.wired.com/story/monero-privacy/> (Accessed 10.07.2024).

¹³ **Forgang**, p. 5.

controversial, legitimate.¹⁴ However, today, the number of altcoins traded on crypto asset exchanges is expressed in the thousands.

Structure of Crypto Assets

Crypto asset units operate in a global, permanent, and censorship-resistant digital environment that uses cryptographic principles to ensure the integrity and speed of transactions, even without the involvement or oversight of trusted third parties. These crypto assets rely on public and private keys developed for peer-to-peer (“P2P”)¹⁵ value transfer, and each transfer is cryptographically signed. The transactions are then verified through a consensus mechanism of a replicated and shared data structure (blockchain technology). Additionally, due to the decentralized nature of crypto assets, there is no central intermediary, such as a bank, responsible for overseeing transactions, being held accountable, or reporting suspicious transactions to relevant authorities. In essence, crypto assets operate on Distributed Ledger Technology (DLT) based on anonymous users and decentralized governance, without any accountability or the need for permission from any authority. Compared to traditional payment methods, the decentralized and anonymous nature of crypto assets makes them more susceptible to abuse and increases their potential use for laundering proceeds of crime.¹⁶ The borderless, P2P nature of crypto assets is said to allow the instantaneous transfer of various funds in a way that the current AML (Anti-Money Laundering) and CFT (Countering the Financing of Terrorism) frameworks cannot trace or prevent. This risk arises because P2P crypto transactions do not require personal identity verification, as there are no real names associated with the addresses of the crypto asset wallets belonging to senders or receivers. Considering the above points, it is evident that the priority level of this risk is high.¹⁷

We can summarize the structure and operation of crypto assets by comparing them to the traditional financial system using the following example:

In the traditional financial system, both X and Y rely on their respective banks (Bank A and Bank B). In this system, transferring funds requires X to identify both Y’s bank and Y’s account identifier. The next step involves X informing their bank that they

¹⁴ **Forgang**, p. 6.

¹⁵ “Peer-to-peer (P2P) technology is a network protocol used to share data between two or more clients. Peers can make a portion of their resources, such as processing power, disk storage, or network bandwidth, directly available to other network participants without the need for centralized coordination by servers or fixed computers. Unlike the traditional client-server model, where servers act as providers and clients as consumers, peers are both providers and consumers. Individuals who wish to buy or sell cryptocurrency often turn to networks of individuals known as peer-to-peer converters or traders.” **Balcı/Çakır**, p. 316.

¹⁶ FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks Report, June 2014, p. 9.

¹⁷ **Christopher P. Buttigieg/Christos Efthymiopoulos/Abigail Attard/Samantha Cuyle**, “Anti-Money Laundering Regulation of Crypto Assets in Europe’s Smallest Member State,” *Law and Financial Markets Review*, Vol. 13, No. 4, 2019, p. 212, 213.

want to transfer money to Y's account. X's bank checks this transaction, and if it is valid, the specified amount is debited from X's account and transferred from Bank A to Bank B. Y's bank then credits this amount to Y's account. In this method, both Bank A and Bank B maintain ledgers capable of controlling the transaction, and all transactions are recorded and stored in these ledgers (nowadays as digital records). Since each bank can report both X's and Y's transactions as well as any unusual transactions that may occur, this method is extremely important and useful for criminal investigations.

However, in the 1990s, when the internet was just becoming widespread and accessible to the public, cyberpunks began questioning the necessity of banks acting as intermediaries and the profits they generated from transactions. Their approach was to use a blockchain, a public ledger, and then sign transactions with public key encryption. Miners (individuals performing mathematical operations for verification and earning a certain amount of crypto assets as a reward) would then compete to reach a consensus for the latest transactions and add a new block to the blockchain for the winner. In Bitcoin's infrastructure, a private key is created for both X and Y, followed by the derivation of an associated public key. This public key is then used to generate a public identity address for transactions. When X wants to send some money to Y, they locate Y's public address and then create a transaction to send a certain amount of Bitcoin to that address. This transaction is signed with X's private key and then taken by miners, who will aggregate all recent transactions and create a consensus to add the transactions to a new block on the blockchain. Before this happens, it must be verified that X's account has enough Bitcoin to pay Y. This verification is why transactions are public: If X does not have sufficient funds to pay Y, miners cannot complete the transaction. Then, a pseudonym is used to match X and Y with a general address. While it is challenging to match these identifiers, law enforcement can at least track known addresses associated with transactions. The concern with this model is that funds may never reach a bank account unless they are converted into fiat currency. This raises concerns for both tax authorities and law enforcement. Consequently, many governments around the world want to regulate crypto assets to monitor fund flows. However, there is also concern that excessive regulation could hinder the emergence of new technologies.¹⁸

This operation can also be described as follows: While the public keys of all transactions are stored on the blockchain, they are not linked to the identity of any individual. Security experts refer to this as pseudonymous privacy, similar to publishing a book under a pseudonym. As long as the pseudonym is not linked to you, your privacy is preserved. However, the trick is exposed the moment someone links

¹⁸ **Simon Dyson/William J. Buchanan/Liam Bell**, "The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime", *The Journal of British Blockchain Association*, Volume 1, Issue 2, 2018, p. 1, 2.

one of your books to you. In doing so, everything the author has written under the pseudonym becomes publicly accessible.¹⁹

Is Possessing, Buying, or Selling Crypto Assets a Crime?

The issuance, possession, and trading of assets we examine under the crypto heading (Bitcoin, Ethereum, Monero, Zcash, etc.) are not unlawful and do not constitute a crime (at least in Türkiye). However, it must be noted that activities in this regard should comply with the regulations introduced by Law No. 7518 dated 26.06.2024 and the Capital Markets Law No. 6362 dated 06.12.2012. Particularly, intermediary institutions (crypto asset service providers) that describe themselves as “Crypto Asset Exchanges” must act in accordance with these regulations. Failure to comply may result in liability for damages, administrative penalties, or criminal offenses. However, as we will discuss below, this regulation applies to intermediary institutions; the crypto assets themselves have not been regulated “by their nature”. Therefore, since a subject not explicitly prohibited by a legal norm is considered permissible, owning and transacting with crypto assets is entirely lawful.

Another point to consider on this matter is that the use of these assets as a payment instrument is prohibited in Türkiye. According to the “Regulation on the Non-Use of Crypto Assets in Payments”, published in the Official Gazette dated 16.04.2021 and numbered 31456, the use of crypto assets in payments is prohibited. In line with this regulation, it is forbidden to use crypto assets directly or indirectly for payments and to provide services for such purposes. In this context, payment service providers are prohibited, under the aforementioned regulation, from developing business models in which crypto assets are directly or indirectly used in the provision of payment services and electronic money issuance, as well as offering any services related to such business models.

Therefore, as long as the Capital Markets Law and the “Regulation on the Non-Use of Crypto Assets in Payments” are complied with, possessing and using these assets is not unlawful and does not constitute a crime. The use of crypto assets in unlawful activities, particularly in the commission of certain economic crimes, does not inherently render their issuance, possession, or use unlawful.

Although possessing and transacting crypto assets is not a crime, understanding why these assets are often associated with various crimes requires examining the similarities and differences between crypto assets and fiat money. In reality, fiat money, particularly in cash form, is largely anonymous (it can only be traced through serial numbers) and has traditionally played a significant role in facilitating crime and illegal trade. The fundamental difference between the two is that crypto assets enable

¹⁹ **Llambi Prendi/Daniel Borakaj/Klarida Prendi**, “The New Money Laundering Machine Through Cryptocurrency: Current and Future Public Governance Challenges”, *Corporate Law & Governance Review*, Vol. 5, Issue 2, 2023, p. 89.

anonymous digital transactions and e-commerce without revealing the identity of the parties involved. This level of anonymity is much harder to achieve with fiat money today due to the heavy regulation of the financial sector. Criminals quickly recognized the anonymity provided by cryptocurrencies. The digital payment systems and e-commerce that emerged as a result of the IT revolution have transformed retail and wholesale trade. Online shopping has significantly influenced the structure of retail, consumption patterns, choice, marketing, competition, and ultimately supply and demand. The impact of this digital revolution in trade was largely limited to legal goods and services until the emergence of blockchain technology and, consequently, crypto assets. This is because digital payments in trade without crypto assets can be easily tracked. However, crypto assets have combined the anonymity of cash with digitalization, changing this dynamic. They have made efficient, anonymous, online, and cross-border trade possible, leading to a significant structural shift in the functioning of the black market, where crypto assets are used to trade illegal goods and services.

The Use of Crypto Assets as Tools for Committing Crimes and Methods

1. Use as a Tool

As a rule, the possession and use of crypto assets do not constitute a crime. However, this does not mean that these assets cannot be used for committing crimes. These tools can be used in the commission of many crimes, especially those motivated by economic gain. The frequent association of crypto assets with various crimes in Türkiye in recent days is for this very reason.

In blockchain technology, tracking fund movements and identifying the individuals behind these transactions is extremely challenging. As a result, some criminals seeking to conduct illegal activities anonymously and covertly have turned to crypto assets to carry out their operations. Crypto assets can be used not only for laundering proceeds of crime but also as tools for payments, storage, or laundering in crimes such as cyber theft, drug trafficking, smuggling, child pornography, and prostitution. Therefore, the use of crypto assets in committing crimes, laundering proceeds of crime, and financing terrorism is a potential risk. The terms “crypto crime,” “cryptocurrency crimes,” and “crypto currencies related crimes” are used to describe crimes committed with crypto assets. These assets are utilized as tools for committing crimes and as alternatives to traditional money because they offer features such as anonymity, decentralization (and thus lack of oversight), and the absence of intermediaries, which are attractive to criminals. Thus, there is no separate type of crime called “crypto asset crime”; rather, the use of these assets in crimes represents a new method (or model) of committing

the crimes I have mentioned.²⁰ For this reason, I believe the term “crimes committed with crypto assets” is more accurate.

Crypto assets are more frequently and commonly associated with crimes such as money laundering and the financing of terrorism, as mentioned above.²¹ The reason for this is the features these tools offer, such as anonymity and difficulty of tracking, which are essential for laundering operations. Indeed, there are significant concerns that the anonymity provided by crypto assets and the lack of regulation facilitate money laundering, tax evasion, drug trafficking, and other criminal activities.²² Another important factor is that transactions made with crypto assets do not fall under the jurisdiction of a single authority and lack a centralized intermediary. This creates a legal ambiguity that makes it difficult to properly control, record, investigate, and prosecute criminal activities stemming from this technological innovation.²³ As can be expected, this environment presents an unparalleled opportunity for criminals, particularly those involved in cybercrimes and economic offenses such as money laundering.

The main reason crypto assets are used to facilitate money laundering is the semi-anonymity they provide to users. This anonymity stems from the fact that, unlike bank accounts, crypto asset addresses are not registered in the name of individuals.²⁴ Crypto asset transaction identities are semi (pseudo) anonymous; while they are not explicitly linked to real-world individuals or entities, all transactions are fully transparent and thus traceable. However, it is very difficult to establish a connection to a real person.²⁵ The blockchain acts as a ledger that replaces a trusted third party by recording every transaction. Each new Bitcoin transaction adds and records a new block to the chain. Although the blockchain is public and transparent, it is considered highly secure,

²⁰ **Murat Volkan Dülger/Onur Özkan**, “Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi”, Prof. Dr. Mehmet Emin Artuk’a Armağan, Ed. Mahmut Koca, Seçkin Yayıncılık, Ankara, 2020, p. 977, 978.

²¹ “It is stated that the use of blockchain in the financing of terrorism is, as far as is known, not very widespread and its share is low. Although there is no evidence of widespread use of Bitcoin and other cryptocurrencies, there are strong indications of their involvement in a series of terrorist attacks in Europe and Indonesia. During the 2021 United Nations Counter-Terrorism Week meetings, it was also emphasized that terrorist organizations have increased their fundraising opportunities by focusing on digital financing. While cryptocurrency technologies are not widely used due to the high level of technical expertise they require, it is expressed that if terrorist organizations enhance their technical capacity to use these technologies, there will likely be an increase in the use of cryptocurrencies in the financing of terrorism.” **Akbulut**, p. 510.

²² **Garry Jacobs**, “Cryptocurrencies & The Challenge of Global Governance”, *Cadmus*, Vol. 3, Issue 4, May 2018, (Online) <https://cadmusjournal.org/>, (Accessed) 11.07.2024

²³ **Elliott Maurice Nathaniel Keech**, “Crime, Innovation, and The Technology of Moneys”, Unpublished PhD Thesis, University of York, York Law School, York, 2022, p. 47, 48.

²⁴ **Rolf van Wegberg/Jan-Jaap Oerlemans/Oskar van Deventer**, “Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin”, *Journal of Financial Crime*, Vol. 25 Issue 2, 2018, p. 422.

²⁵ **Sarah Meiklejohn/Marjori Pomarole/Grant Jordan/Kirill Levchenko/Damon McCoy/Geoffrey M. Voelker/Stefan Savage**, “A Fistful of Bitcoins: Characterizing Payments among Men with No Names”, *Communications of the ACM*, Vol. 59, Issue 4, Nisan 2016, p. 86.

contrary to what might be assumed.²⁶ Blockchain technology creates a transaction archive known as Distributed Ledger Technology (DLT), where a copy of every transaction block is distributed and made visible to all network members.²⁷ Individuals and criminal organizations can use different pseudonyms to hide their real identities, enabling transactions to be conducted semi-anonymously and making it very difficult to trace the real individuals behind them. Additionally, crypto assets do not need to be transferred through a bank or a trusted third party. Instead, crypto assets can be moved freely and independently.²⁸

Compared to traditional currencies, crypto assets allow for greater anonymity because parties conducting transactions on the public ledger are identified only by their public keys, and the distributed ledger technology on which crypto assets operate permits anonymous funding (cash funding or third-party funding through virtual converters that do not accurately identify the source of funds). In addition, it allows anonymous transfers where the sender and recipient of the funds are not sufficiently identified, which is critical from a KYC (Know Your Customer) perspective.²⁹ Furthermore, certain developments in crypto asset technology make tracking fund transfers even more difficult. For instance, while there are some blockchain analysis tools available to remove the anonymity of Bitcoin and certain altcoin transactions, privacy assets (Monero, ZCash, Dash), off-chain channels (e.g., Lightning Network, Raiden, Plasma, etc.), and mixers/tumblers (e.g., Shapeshift) pose significant challenges for KYC compliance. Although privacy assets operate using open-source public DLTs, they do not offer the same visibility or identifying details. For example, Monero does not provide visibility into the sender, recipient, or value of transactions on its DLT. It employs stealth addresses or newly created one-time-use addresses to ensure that only the sender and recipient can access transaction details. Additionally, it creates ring signatures, which enable transactions to be signed among a group of users, thereby preventing attribution of the signature to individual users. On the other hand, ZCash offers optional privacy and incorporates the “zero-knowledge proof”³⁰ feature, which ensures the legitimacy of transactions on the ZCash network by allowing parties to reach consensus on the validity of information while keeping the identities of the other parties encrypted and protected.³¹

For this reason, crypto assets create new opportunities for criminals that are more difficult for regulatory bodies to control. The semi-anonymity provided by crypto

²⁶ Balcı/Çakır, p. 315, 316.

²⁷ David Yermack, “Corporate Governance and Blockchains”, *Review of Finance*, Vol. 21, Issue 1, March 2017, p. 17

²⁸ Forgang, p. 6, 7.

²⁹ FATF, *Virtual Currencies Key Definitions and Potential AML/CFT Risks Report*, June 2014, 9.

³⁰ Zero-knowledge proof is a method in which a person confirms to another that they possess certain information without granting direct access to that information.

³¹ Buttigieg/Efthymiopoulos/Attard/Cuyle, p. 213.

assets is increasingly being used for invisible illegal transactions, money laundering, and the financing of terrorism.³² However, the frequent association of crypto assets with laundering and financing terrorism does not mean that the majority of laundering activities are carried out with crypto assets, or that money laundering started or increased with the advent of crypto assets.³³ The practice of money laundering did not emerge with the discovery of blockchain technology or its application to Bitcoin and other altcoins.³⁴ In fact, the history of money laundering dates back to the early 20th century, long before the invention of the computer.

The frequent association of crypto assets with money laundering is primarily due to two features provided by blockchain technology: The decentralized (distributed) structure of transactions in global networks and the semi-anonymity it offers. These features have enabled the emergence of new methods for laundering proceeds of crime on an international scale.³⁵ In this context, crypto assets can be used in all three stages of the money laundering process due to the features provided by blockchain technology:³⁶

a) Placement Stage: When proceeds of crime are converted into crypto assets instead of cash or other financial instruments, the peer-to-peer (P2P) transaction feature enabled by blockchain technology—allowing parties to transact directly without the need for intermediaries or verification—helps bypass the strict oversight of banking and financial systems.³⁷ The placement stage involves purchasing primary crypto assets (e.g., Bitcoin, Ethereum, Litecoin) using cash or a bank card through a crypto asset exchange or mostly unregulated crypto ATMs. At this stage, “straw men” (individuals who are not the actual beneficiaries of the transaction but possess clean records and verified information) are often used to pass KYC verification at intermediary institutions. Illegal actors may also attempt to clean funds originating from unlawful sources by purchasing crypto assets during an Initial Coin Offering (ICO). An added advantage of coins purchased from an ICO is that they are newly minted, eliminating the risks associated with transaction history. During this stage, the

³² Keech, p. 54; Çakır, p. 77

³³ Ole Bjerg, “How is Bitcoin Money?”, *Theory, Culture & Society*, Vol. 33, Issue 1, 2016, p. 53-72.

³⁴ Malcolm Campbell-Verduyn/Marcel Goguen, “The Mutual Constitution of Technology and Global Governance: Bitcoin, Blockchains, and the International Anti-money-laundering Regime”, in: *Bitcoin and Beyond Cryptocurrencies, Blockchains, and Global Governance*, Ed. Malcolm Campbell-Verduyn, Routledge, London and New York, 2018, p. 72; Bjerg, p. 53-72; Forgang, p. 14.

³⁵ Campbell-Verduyn/Goguen, p. 74

³⁶ Balci/Çakır, p. 324.

³⁷ Erdal Durdu, *Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku*, Unpublished Master’s Thesis, Galatasaray University, 2018, p. 189; Campbell-Verduyn/Goguen, p. 74; Dülger/Özkan, p. 989.

“smurfing”³⁸ method is often used to divide the funds into small, insignificant amounts and spread them across different locations.³⁹

b) Layering Stage: In this stage, the relationship between crypto assets and the source of proceeds of crime can be severed, and their traceability obscured by conducting complex fund movements known as “mixing”, which prevents identity tracking and combines transactions in unpredictable ways.⁴⁰ Blockchain technology and the execution of the layering stage using crypto assets through computer systems provide various opportunities for offenders.⁴¹ The layering stage is the most complex stage as it consists of numerous and diverse transactions designed to obscure the source of funds and avoid detection. To conceal the traces of primary crypto assets, techniques such as mixing or tumbler services are used to replace primary addresses with temporary wallet addresses, thereby preventing regulatory bodies from tracking these transactions. Another method involves deliberately falsifying recipient addresses to redirect transactions to backup addresses, thus corrupting the audit ledger. The mixed primary crypto assets are then transferred to a crypto asset intermediary (e.g., Kraken, Binance, Coinbase) to purchase privacy assets. Illegal funds or proceeds of crime are effectively cleaned and prepared for integration into the traditional financial system by layering multiple privacy assets, exchanges, and digital addresses, making their tracking significantly more difficult.⁴²

c) Integration Stage: When the assets derived from crime are held as crypto assets, as mentioned above, these assets can be used to purchase real and/or virtual goods and services or converted into fiat currencies at exchange centers. In this way, it becomes possible to integrate the assets derived from crime into the financial system through legitimate transactions.⁴³ During the integration stage, there are various options for withdrawing cleaned funds from crypto assets to obtain fiat currency. These include exchanging privacy assets for primary assets and eventually for fiat currency or transferring crypto assets to a hardware crypto wallet for physical transportation to any desired location.⁴⁴ Thus, crypto assets serve all three stages of money laundering.

Criminals, particularly those who derive proceeds from cybercrimes, require a secure cash-out strategy to launder these proceeds, specifically crypto assets in this context. An individual who has committed a cybercrime and seeks to launder the resulting proceeds rarely begins the cash-out process with crypto assets. Such proceeds typically

³⁸ Smurfing is a method that involves using several individuals to carry out transactions on behalf of and for the benefit of the primary person laundering the proceeds of crime. Detailed explanations regarding the smurfing method are provided in the following pages.

³⁹ Buttigieg/Efthymiopoulos/Attard/Cuyle, p. 214.

⁴⁰ Campbell-Verduyn/Goguen, p. 80; Durdu, p. 189.

⁴¹ Dülger/Özkan, p. 989.

⁴² Buttigieg/Efthymiopoulos/Attard/Cuyle, p. 214.

⁴³ Durdu, p. 190; Dülger/Özkan, p. 989.

⁴⁴ Buttigieg/Efthymiopoulos/Attard/Cuyle, p. 214.

consist of fiat currencies like euros or dollars. Regardless of the source, nature, or size of the proceeds from cybercrimes, the crypto asset ecosystem is used as part of the anonymization or layering process required by the cash-out strategy. When these proceeds are exchanged for crypto assets, particularly Bitcoin, the trace of the money is effectively erased.⁴⁵

The methods that can be used to launder crypto assets are extensive and often complex, particularly the layering process, which poses significant challenges for AML/CFT authorities. Despite this, tools aimed at overcoming these regulatory hurdles are continuously being developed.⁴⁶

2. Methods

When criminals engage in laundering activities using crypto assets, they often employ various methods such as crypto asset tumblers, mixing services, peer-to-peer (P2P) networks, OTC brokers, and the exploitation of DeFi platforms. Although their approaches differ, all these methods serve the same purpose: To obscure the original source of illicit proceeds and make it harder for law enforcement to trace them. For instance, crypto asset mixers and mixing services break down large amounts of crypto assets into smaller, untraceable amounts. Similarly, peer-to-peer networks and OTC brokers provide platforms for anonymous transactions, further complicating the tracking process. Finally, the exploitation of DeFi platforms takes advantage of the lack of regulation and oversight in the crypto sector, allowing criminals to move funds through complex transaction networks. Each of these methods poses challenges for law enforcement and highlights the need for the continuous development of advanced tools and techniques to combat the laundering of crypto assets.⁴⁷

Crypto Asset Tumblers and Mixing Services

Crypto asset tumblers and mixing services⁴⁸ play a central role in many laundering operations. These services help criminals obscure the origin of illicit proceeds by breaking them into smaller amounts, processing them through a series of transactions, and then recombining them. As a result of these processes, a series of funds is created that is difficult to trace back to its original source, making it challenging for law enforcement to identify and prosecute offenders. The use of tumbling and mixing

⁴⁵ van Wegberg/Oerlemans/van Deventer, p. 420.

⁴⁶ Buttigieg/Efthymiopoulos/Attard/Cuyle, p. 214.

⁴⁷ Financial Crime Academy, "Understanding Crypto Money Laundering Methods: The Cryptocurrency Crime", (Online) [https://financialcrimeacademy.org/cryptocurrency-money-launderingmethods/#:~:text=What%20are%20the%20methods%20of,decentralized%20finance%20\(DeFi\)%20platforms.](https://financialcrimeacademy.org/cryptocurrency-money-launderingmethods/#:~:text=What%20are%20the%20methods%20of,decentralized%20finance%20(DeFi)%20platforms.) (Accessed) 10.06.2024.

⁴⁸ For an experimental and empirical study on mixing services, see. Malte Möser/Rainer Böhme, "Anonymous Alone? Measuring Bitcoin's Second-Generation Anonymization Techniques," 2017 IEEE European Symposium on Security and Privacy: Workshops (EuroS&PW), 2017, pp. 32–41; see also. van Wegberg/Oerlemans/van Deventer, p. 420 et seq.

services is not limited to money laundering; they can also be used to facilitate other criminal activities, such as drug trafficking and cybercrimes.⁴⁹

The first-generation crypto asset mixers operated as centralized services for mixing. These were the oldest and most rudimentary services for mixing crypto assets. The success of anonymization through such services depended on the number of users and the amount of crypto assets involved. For this reason, these dedicated services were not very popular. Crypto asset intermediaries and other trading platforms are more commonly used for similar purposes.

If a mixer is sufficiently large, the deposited funds are ultimately converted into other crypto assets, and it is not even necessary to sell or buy them. In this way, crypto assets are effectively mixed without commission. However, such a service must be reliable. The providers of mixing services must not take ownership of the crypto assets themselves, and these assets must be protected against external thefts and system breaches. Additionally, there must be complete trust that the service does not record, sell, or share reports of the mixing transactions. Even if the mixer guarantees the return of crypto assets to their owner, it is still challenging to ensure all of the above conditions simultaneously and to alleviate all concerns.⁵⁰

Nevertheless, it should be noted that this method is quite effective. For instance, it has been reported that the tumbler application *Helix* mixed approximately \$300 million worth of Bitcoin in an inseparable manner, thereby facilitating the laundering of proceeds of crime.⁵¹ However, in accordance with FATF's Recommendation 15, countries are required to impose various obligations on such service providers, take measures to pierce the veil of anonymity, and develop software capable of tracking open-source blockchain transactions to identify the individuals behind them. Due to these efforts, the global average of illicit funds used on direct exchange platforms decreased by 47% in 2019.⁵²

Peer-to-Peer Networks, OTC Brokers, and Off-Chain Channels

Peer-to-peer networks and OTC⁵³ brokers provide another means for criminals to launder proceeds of crime through crypto assets. These platforms allow users to trade crypto assets without disclosing their identities, offering an environment where

⁴⁹ **Financial Crime Academy**, Crypto Money Laundering.

⁵⁰ **Sat/Krylov/Bezverbnji/Kasatkin/Kornev**, p. 246; **Prendi/Borakaj/Prendi**, p. 85.

⁵¹ **Zeynep Esra Tarakçıoğlu**, "Kripto Varlıkları ve Ceza Hukuku Sorumluluğu", *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi*, Vol. 11, Issue. 2, December 2021, p. 342.

⁵² **Cipher Trace**, Cryptocurrency Crime and Anti Money Laundering Report, 2020, p. 7.

⁵³ OTC (Over the Counter) refers to over-the-counter markets, which are non-exchange markets. They are not organized markets like BIST, Nasdaq, or NYSE. These markets operate under more relaxed rules and oversight. In these markets, buyers and sellers conduct transactions directly without any intermediaries.

criminals can operate relatively anonymously. By using these platforms, criminals can launder proceeds of crime without leaving any trace that could lead to their detection.

To address this issue, regulatory agencies must ensure that peer-to-peer networks and OTC brokers implement strict KYC/AML⁵⁴ policies. FATF's guidelines explain what these measures should entail. Indeed, states and financial institutions have taken several steps to combat criminal activities related to crypto assets. These steps include anti-money laundering (AML) regulations aimed at stopping money laundering and terrorist financing, as well as "Know Your Customer" (KYC) standards that require financial institutions to verify the identities of their customers.⁵⁵ According to Article 3 of Law No. 5549, obligated parties must first identify the individual performing the transaction and the person on whose behalf the transaction is being conducted and take necessary precautions for the transactions they handle or mediate.⁵⁶ By implementing these measures, these platforms can help prevent money laundering and other illegal activities while also protecting their users from potential risks. Additionally, law enforcement agencies should collaborate with the operators of these platforms, sharing information and resources, to facilitate the detection and prevention of criminal activities.⁵⁷

In off-chain channels (e.g., Lightning Network, Raiden, Plasma, etc.), transactions are conducted through an opened payment channel, allowing them to continue without the need to be published on the blockchain.⁵⁸

Exploitation of Decentralized Finance (DeFi) Platforms

Decentralized Finance (DeFi) platforms have emerged as a new opportunity in the crypto space by offering a range of innovative financial products and services. However, the lack of regulation and oversight in the DeFi sector has made it attractive to those seeking to launder proceeds of crime. Criminals exploit the anonymity and decentralization offered by these platforms to move illicit proceeds through complex transaction networks, making it difficult for law enforcement to trace their origins. To combat the use of DeFi platforms for money laundering purposes, regulatory agencies must develop and enforce appropriate regulations and oversight mechanisms. They should ensure that DeFi platforms operate transparently and securely while protecting users from potential risks associated with money laundering and other illegal activities.⁵⁹

⁵⁴ Know Your Customer/Anti Money Laundering

⁵⁵ **Prendi/Borakaj/Prendi**, p. 85.

⁵⁶ **Balcı/Çakır**, p. 327.

⁵⁷ **Financial Crime Academy**, Crypto Money Laundering.

⁵⁸ **Buttigieg/Efthymiopoulos/Attard/Cuyle**, p. 213.

⁵⁹ **Financial Crime Academy**, Crypto Money Laundering.

3. The Role of Methods in Committing Crimes

These methods provide two main advantages to launderers. These are the ability to bypass trusted intermediaries, such as banks at the core of the AML regime, and the provision of semi-anonymity to users. In money laundering, it is crucial for both the individual generating the proceeds and the one conducting the transactions to remain anonymous. This ensures that the link between the proceeds and the crime is severed, eliminating the risks of identifying the perpetrators and confiscating the proceeds of crime. At this point, the semi-anonymity provided by crypto assets offers significant opportunities to launderers, making it much easier to launder proceeds of crime using crypto assets.⁶⁰ Blockchain technology is semi-anonymous because every transaction made on the blockchain can be seen on all computers where it is stored, and the chain of transactions can be traced from start to finish. In this sense, it is entirely transparent. On the other hand, the individuals conducting these transactions are identified only by numbers and pseudonyms. Since no central authority keeps records, there is no need or ability to determine the true identities of individuals. The identical record of the transaction, which ensures its security, is stored on every computer—essentially making the transaction itself the record. This combination of transparency and anonymity creates a semi-anonymous state. This semi-anonymity provides excellent opportunities for those wishing to conduct financial transactions while remaining hidden. However, these opportunities present significant challenges for those combating crime.

As a result, blockchain technology, which enables direct transactions between users on networks that can be widely used worldwide but lack a central structure and regulator, bypasses trusted third parties such as banks at the heart of the international AML regime. It helps evade the AML controls applied through these institutions. In traditional centralized systems, verifying and monitoring the exchange of funds relies on trusted financial institutions like banks. In transactions made with crypto assets, however, trust is placed in complex algorithms and decentralized networks of users that continuously verify the validity of transactions. Thus, crypto assets allow users to transfer funds directly among themselves (P2P = peer-to-peer) without the involvement of traditional trusted third parties. Since no third party is involved in fund transfers or conversions, oversight through such an intermediary becomes impossible. This is significant because financial institutions are the primary structures targeted by and effective under the KYC/AML regime. When these institutions are removed, the application of the KYC/AML regime becomes nearly impossible. It is noted that, due to the lack of central institutions ensuring compliance with international AML requirements, blockchain applications like crypto assets have “*effectively*

⁶⁰ van Wegberg/Oerlemans/van Deventer, p. 432.

circumvented many anti-money laundering regulations developed over the last 25 years.”^{61,62}

Another feature of blockchain technology that impacts the international AML regime, as mentioned earlier, is the semi-anonymity it provides to users. The conflict between the desire for transparency and anonymity is a fundamental issue faced by digital technologies in general, and it is particularly evident in blockchain applications. Blockchain serves as a digital ledger where crypto assets are created, transferred, or stored. Crypto assets use cryptography through the blockchain system.⁶³ Identifying the real-world identities of individuals based on user addresses is difficult, though not impossible, due to the complexity of the cryptographic methods underlying blockchain. This semi-anonymity makes it challenging for financial institutions’ employees to determine exactly whom to question. In connection with this, financial professionals and sector regulators need to develop an understanding of which crypto asset transactions are “atypical” and which are “normal.” In this context, it is essential for financial professionals and regulatory bodies to recognize what exactly a suspicious Bitcoin transfer looks like. In other words, a standard reference must be established regarding the typical uses of suspicious blockchain-based crypto asset transactions.⁶⁴

In conclusion, the decentralized structure of blockchain technology and its ability to provide semi-anonymity have significant implications for the international AML/CFT regime. Blockchain-based transactions, such as those involving crypto assets, do not rely on or use traditional banks and financial institutions as “common trust and transition points” for fund transfers. Instead, they enable direct peer-to-peer transactions, with the technology itself being built to provide this trust. As a result, the ability to identify the parties involved in blockchain-based transactions is significantly reduced.⁶⁵

The Potential Use of Crypto Assets in Money Laundering and Striking Examples

The emergence of crypto assets has brought new opportunities for investment in the financial sector. However, this development has also created new opportunities for criminals to launder proceeds of crime through this digital environment and crypto assets. Although the full scale of crypto asset misuse is not known, the market value of all circulating crypto asset units worldwide exceeded \$250 billion in 2020 and reached approximately \$1.94 trillion in 2022.⁶⁶ Moreover, it is estimated that in 2022,

⁶¹ **Robert Stokes**, “Anti-money Laundering Regulation and Emerging Payment Technologies”, in: Banking and Financial Services Policy Report, Vol. 32, Issue. 5, 2013, p. 3.

⁶² **Campbell-Verduyn/Goguen**, p. 74.

⁶³ **Akbulut**, p. 489.

⁶⁴ **Stokes**, p. 5; **Campbell-Verduyn/Goguen**, p. 74.

⁶⁵ **Campbell-Verduyn/Goguen**, p. 75.

⁶⁶ **Keech**, p. 48.

crypto assets worth \$23.8 billion were used in illegal activities, and this amount is steadily increasing.⁶⁷ Additionally, the revenue in the crypto asset sector reached approximately \$42 billion in 2023, and it is expected to grow at an annual rate of 14.36% by 2027. User penetration is reported to be 3.8% in 2023 and is expected to rise to 4.4% by 2027.⁶⁸ As seen, the figures are remarkably high and are accelerating with each passing day.

It is estimated that illegal users control approximately 39.31% of crypto asset addresses and account for about one-fifth (23.06%) of the dollar volume of crypto asset transactions. In dollar terms, it is claimed that illegal users have conducted crypto asset transactions worth approximately \$429 billion. Since illegal users hold a larger share of transactions than their dollar volume share, they tend to make smaller transactions compared to legitimate users. This finding aligns with the claim that illegal users primarily use crypto assets as a payment system—therefore, as a payment instrument for committing crimes or for laundering proceeds of crime—rather than holding them as an investment or speculative asset.⁶⁹

As previously mentioned, one of the most significant and real examples of the potential use of crypto assets in money laundering is the online marketplace *Silk Road*, which operated on the “dark net”, accepted only Bitcoin for transactions, and led to its creator, Ross Ulbricht, being sentenced to life imprisonment for money laundering and other crimes.⁷⁰ *Silk Road* has become the most prominent and well-known example of Bitcoin being used in illegal activities to prevent criminals from being caught. Another method of laundering with crypto assets and a case that was uncovered involves using multiple individuals to conduct transactions on behalf of and for the benefit of a primary person laundering proceeds of crime. This method is known as “smurfing”. The logic behind smurfing is that several individuals conducting small transactions in different locations draw far less suspicion and attention than a single individual conducting a large transaction. Smurfing is an old method of money laundering, but it has become a global problem due to the ease and speed with which crypto assets can be transferred worldwide. This method was uncovered in a joint investigation

⁶⁷ **Financial Crime Academy**, Crypto Money Laundering.

⁶⁸ **Prendi/Borakaj/Prendi**, p. 85.

⁶⁹ **Foley/Karlsen/Putnins**, p. 24

⁷⁰ *Silk Road* was an online black market and darknet marketplace active in the early 2010s, known for the sale of illegal substances. It played a pivotal role in the emergence of the darknet marketplace. The market, hosted on the deep web, operated on the Tor network with a “.onion” extension, enabling users to access the site anonymously and securely. The site, which was launched in February 2011, had been under development six months prior to its launch. During its active period, over 100,000 customers purchased products available on the platform. In October 2013, the FBI seized and shut down the site and arrested *Ross Ulbricht*, accusing him of being the founder, known as “Dread Pirate Roberts”. The following month, a site called *Silk Road 2.0* was launched, but it too was shut down in November 2014 during an operation called *Operation Onymous*, and its administrator was arrested. In 2016, *Silk Road 3.0* was created, but it failed to regain the popularity of its predecessors due to competition from other sites. *Ulbricht* was sentenced to life imprisonment without the possibility of parole for his involvement with the site. In November 2020, the U.S. government announced that they had seized bitcoins worth \$1 billion related to *Silk Road*. ([Online](#), accessed 04.07.2024).

conducted by Europol, the Spanish Civil Guard (*Guardia Civil*), Finnish law enforcement, and the U.S. Department of Homeland Security. The investigation revealed a complex global smurfing scheme that resulted in the arrest of 11 individuals and the seizure of 8 million euros. This method initially involved criminals based in Spain, who were tasked with collecting proceeds from illegal drug trafficking and distributing them among 174 different bank accounts. The criminals later traveled to Colombia, where they withdrew the money from these accounts using bank cards linked to them. However, when the criminals realized their actions could be easily traced through transaction histories, the plan shifted to using Bitcoin and other cryptocurrencies for laundering instead of cash. Instead of withdrawing the cash themselves, the criminals used intermediary institutions to convert the illicit proceeds deposited in accounts into crypto assets. They then converted the cryptocurrencies into Colombian pesos and deposited them into Colombian bank accounts on the same day. The plan was uncovered after authorities identified the location of the crypto asset intermediary and collected all the personal identification information the intermediary had about the suspects.⁷¹ Some studies have found a correlation between the use of crypto assets and illegal activities by analyzing U.S. search engine data.⁷² However, apart from these examples, there is limited evidence directly linking blockchain applications to actual money laundering operations. For instance, the 2015 UK National Risk Assessment Report concluded that there were “a limited number of case studies that could lead to concrete findings regarding the use of digital currencies for money laundering” and that “the money laundering risk associated with digital currencies was low”.⁷³

Despite sensational media reports, there is very little evidence to suggest that crypto assets are used for financing terrorism. Claims that the perpetrators of the November 2015 terrorist attacks in Paris used crypto assets have been proven unfounded. While there is a theoretical risk of crypto assets being used for money laundering and terrorism financing, it has not yet been concretely demonstrated that they are used for such purposes.

According to a 2018 report on money laundering by the crypto asset security firm *CipherTrace*, there are between 100 and 200 gambling websites on the internet that allow gambling with crypto assets.⁷⁴ Similar to a regular casino, funds can be transferred to an online casino for betting purposes, but they can also be withdrawn without playing a significant number of bets or spending a substantial amount of

⁷¹ **Europol**, “Illegal Network Used Cryptocurrencies and Credit Cards to Launder More Than EUR 8 Million from Drug Trafficking,” April 9, 2018, ([Online](#), accessed 11.07.2024).

⁷² **Aaron Yelowitz/Matthew Wilson**, “Characteristics of Bitcoin Users: An Analysis of Google Search Data”, *Applied Economics Letters*, Vol. 22, Issue 13, 2015, p. 1-7.

⁷³ See. HM Treasury and Home Office, UK National Risk Assessment of Money Laundering and Terrorist Financing, October 15, 2015, ([Online](#), accessed 05.07.2024).

⁷⁴ **Cryptocurrency Anti-Money Laundering Report**, 2018, ([Online](https://info.ciphertrace.com/crypto-aml-report-q218)) <https://info.ciphertrace.com/crypto-aml-report-q218>, (accessed) 11.07.2024.

money. The report states that the main challenge in tracking money laundering through online casinos is the lack of or minimal implementation of “Know Your Customer” (KYC) regulations on these gambling sites, making it difficult for law enforcement to obtain information about transfers made from these sites.⁷⁵ Even a simple internet search for websites that allow gambling with crypto assets reveals that sites such as <https://bitcoinplay.net> advertise different platforms that can be used for gambling. Furthermore, this website promotes anonymity and potentially allows its platforms to be exploited for money laundering activities.⁷⁶ However, as can be seen, this report also mentions the “potential” use of crypto assets in criminal activities but does not, naturally, provide any numerical data related to this issue.

One of the largest cases in the history of online money laundering is the *Liberty Reserve* incident. In May 2013, the U.S. Department of Justice filed various charges against seven executives and employees of the *Liberty Reserve* company, which operated in Costa Rica. These individuals were accused of engaging in unregistered commercial activities by providing money transfer services and laundering more than \$6 billion in illicit proceeds. According to statements, this system operated on an enormous scale, with millions of users worldwide, including 200,000 users in the U.S. Approximately 55 million transactions were conducted within this system, almost all of which were illegal. The system used its own virtual currency, *Liberty Dollars*. However, at the starting and ending points of transactions, the money was converted and exchanged into fiat currencies (e.g., USD). As a result of well-coordinated actions, the U.S. Department of Treasury designated *Liberty Reserve* as a financial institution of primary money laundering concern and completely blocked its access to the U.S. financial system under Section 311 of the USA Patriot Act.⁷⁷ As seen, a virtual currency valid within a specific system was also used in this case.

Another recent development in this context was Europol’s announcement, first released on January 12, 2021, and updated on November 18 of the same year, stating that it had taken *DarkMarket*, the world’s largest illegal marketplace on the dark web at the time, offline. According to the statement, *DarkMarket* had 500,000 users, 2,400 sellers, and 320,000 unpaid transactions involving 4,650 Bitcoins and 12,800 Moneros, amounting to over €140 million at the exchange rates of that time. In the same press release, Europol emphasized the need for a coordinated law enforcement approach to combat crimes on the dark web as a clear indicator of the scale of this issue.⁷⁸ It was noted that, compared to the overall estimates of crimes committed with crypto assets, this amount was not particularly significant but was likely a substantial

⁷⁵ Cryptocurrency Anti-Money Laundering Report, 2018, p. 9.

⁷⁶ **Forgang**, pp. 15-16.

⁷⁷ **Valeriia Dyntu/Oleh Dykyi**, “Cryptocurrency in the System of Money Laundering”, *Baltic Journal of Economic Studies*, Vol. 4, No. 5, 2018, p. 79.

⁷⁸ (Online) <https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down> (accessed) 18.07.2024

figure in the ranking of amounts seized from individual operations.⁷⁹ Therefore, these illegal marketplaces, or underground markets, can be seen as facilitators for the use of crypto assets in current and future money laundering schemes for illicit proceeds.⁸⁰

The most recent development on this topic occurred in the United States. A dual Russian-Swedish citizen named *Roman Sterlingov*, accused of laundering \$400 million since 2011 through a cryptocurrency mixing service on the darknet, was convicted by a federal jury in Washington for operating a long-running money laundering service on the darknet. Roman Sterlingov ran *Bitcoin Fog*, a cryptocurrency “mixer” service that allowed criminals to launder hundreds of millions of dollars in illicit funds from darknet marketplaces. The defendant and his clients used *Bitcoin Fog* to conceal these illegal transactions. Deputy Attorney General Lisa Monaco stated, “*He thought he could use the shadows of the internet to launder hundreds of millions of dollars in bitcoin without getting caught, but he was wrong; our team of agents, analysts, and prosecutors meticulously followed bitcoin through the blockchain to hold Sterlingov and Bitcoin Fog accountable in their pursuit of justice. Today, the jury found him guilty on all charges—showing that no matter where you operate, if your cryptocurrency service reaches the U.S., you must comply with U.S. law*”. FBI Deputy Director Paul Abbate added, “*The FBI’s cyber workforce remains relentless in its pursuit of criminals who leverage technology to commit and facilitate illegal activities. This conviction is the result of close collaboration between the FBI and federal and international partners, ensuring criminal penalties were imposed on Bitcoin Fog and its operator for money laundering activities. The FBI will continue to use all available tools and resources to hold cybercriminals accountable, wherever they operate*”.

According to court documents and evidence presented at trial, 35-year-old Roman Sterlingov was involved in operating *Bitcoin Fog* from 2011 to 2021. *Bitcoin Fog*, known as the longest-running cryptocurrency mixer, gained a reputation as a money laundering service for criminals seeking to hide illicit proceeds from law enforcement. Over its decade-long operation, *Bitcoin Fog* facilitated more than 1.2 million Bitcoin transactions, worth approximately \$400 million during the transactions. A large portion of this cryptocurrency originated from darknet markets and was linked to illegal narcotics, cybercrimes, identity theft, and child exploitation materials. The jury convicted Sterlingov of “conspiracy to commit money laundering” and “concealed money laundering”, each carrying a maximum penalty of 20 years in prison, and “operating an unlicensed money transmission business” and “unlicensed money transmission” in the District of Columbia, each carrying a maximum penalty of five years in prison. An important aspect of this case and the preceding investigation was the national and international cooperation among institutions that led to the exposure

⁷⁹ **Michele Manna**, *The Bonfire of Banknotes, Mercati, Infrastrutture, Sistemi di Pagamento (Markets, Infrastructures, Payment Systems) Approfondimenti (Research Papers)*, No. 25 Banca d'Italia, Rome, 2022, p. 20.

⁸⁰ **van Wegberg/Oerlemans/van Deventer**, p. 421

of these crimes and the punishment of the perpetrator. The investigation was primarily conducted by the IRS-CI District of Columbia Cyber Crimes Unit and the FBI Washington Field Office. The U.S. Department of Justice's Office of International Affairs and the FBI's Virtual Assets Unit assisted the investigation teams. Additional support was provided by Europol, the Swedish Economic Crimes Authority, the Swedish Prosecution Authority, the Swedish Police Authority, the General Inspectorate of the Romanian Police, the Directorate for Combating Organized Crime, and the Directorate for Investigating Organized Crime and Terrorism.⁸¹

From this perspective, it can be easily stated that estimates regarding money laundering operations conducted using crypto assets are based not on concrete evidence but on various predictions and calculations. It appears that the existing examples are too few to represent the general situation. Indeed, some legal experts have warned that the use of crypto assets in money laundering may be more of a perceived opportunity than a real one.⁸² Similarly, many technology experts argue that the risk of crypto assets being used to launder illicit proceeds is "exaggerated". Nonetheless, key actors in the international AML regime believe that blockchain technologies complicate efforts to prevent money laundering and the financing of terrorism.⁸³

In our opinion, crypto assets have significant potential for use in money laundering. However, this does not mean that this potential has become a reality. The examples we provided above remain minuscule in comparison to the total amount of laundered proceeds globally. Therefore, KYC should be implemented for crypto assets, and the AML/CFT regime should be activated. However, the existence and development of this technology and the crypto asset ecosystem should not be hindered or eliminated solely because of this potential risk. Additionally, it must be acknowledged that banning such technology outright could drive it underground.

FATF's Regulations

The FATF (Financial Action Task Force) is a prominent and leading organization in the global fight against money laundering and the financing of terrorism. Consequently, through its work and guidelines specific to this area, FATF serves as a guide for policymakers and practitioners worldwide in combating money laundering and the financing of terrorism. Leveraging this role and the authority it derives from it, FATF has published various guidelines regarding the use of crypto assets in money laundering and terrorism financing. The conclusion drawn from FATF's guidelines, as explicitly stated by the organization itself, is a "risk-based" approach to crypto assets.

⁸¹ (Online)<https://www.justice.gov/opa/pr/bitcoin-fog-operator-convicted-money-laundering-conspiracy> (Accessed) 18.07.2024.

⁸² **Steven David Brown**, "Cryptocurrency and Criminality: The Bitcoin Opportunity", *The Police Journal*, Vol. 89, Issue 4, 2016, s. 332; Stokes, p. 5.

⁸³ **Campbell-Verduyn/Goguen**, p. 75.

This approach has resonated globally, creating the perception that these risks have already materialized, which has led to crypto assets being associated with money laundering and terrorism financing. However, at present, crypto assets pose less of a threat and more of an opportunity for global efforts to combat these illegal practices.⁸⁴ While a risk-based approach is valid, as we emphasized earlier, it is not a reality that these assets are “used solely for committing crimes”. Therefore, FATF’s approach should be interpreted as addressing potential risks and taking precautions before these risks materialize. However, this does not justify banning crypto assets or even blockchain technology. The development of blockchain technology should not be hindered under the guise of these risks.

FATF first addressed this issue in its report⁸⁵ dated June 2014, where it worked to define virtual currencies and the risks they entail. A year later, in June 2015, it published⁸⁶ a risk-based approach guide for virtual currencies, which was subsequently updated in October 2021.⁸⁷

FATF’s Recommendation 15 was updated in 2019 to apply Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) measures to virtual assets (VAs) and virtual asset service providers (VASPs). According to this:

“15. New Technologies: Countries and financial institutions should (a) identify and assess the risks of money laundering or terrorist financing that may arise in connection with the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and existing products. For financial institutions, such a risk assessment should be conducted before the introduction of new products, business practices, or new and developing technologies. They must take appropriate measures to manage and mitigate these risks.

To manage and mitigate risks arising from virtual assets, countries should ensure that virtual asset service providers are regulated, licensed, or registered for AML/CFT purposes and are subject to effective systems to monitor and ensure compliance with the relevant measures outlined in the FATF Recommendations.”

FATF presented the fifth update on compliance with Recommendation 15 and its Interpretive Note (R.15/INR.15) in a report published in July 2024.⁸⁸ Similarly, the

⁸⁴ **Malcolm Campbell-Verduyn**, “Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance” *Crime, Law and Social Change* V. 69, No. 2, March 2018, p. 299.

⁸⁵ FATF, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, June 2014.

⁸⁶ FATF, *Guidance for a Risk-Based Approach to Virtual Currencies*, June 2015.

⁸⁷ FATF, *Updated Guidance for a Risk-Based Approach to Virtual Currencies* October 2021.

⁸⁸ FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, June 2024. “This report presents the fifth update on the compliance of jurisdictions with FATF Recommendation 15 and its Interpretive Note (R.15/INR.15). Recommendation 15 was updated in 2019 to apply Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) measures to virtual assets (VAs) and

articles added to Türkiye's Capital Markets Law (CML) regulating crypto assets and crypto asset service providers were implemented to ensure compliance with FATF's updated Recommendation 15.

The two fundamental characteristics of blockchain technologies—decentralization and semi-anonymity—have shaped FATF's response, which lies at the heart of the international AML regime. FATF has first highlighted the challenges of monitoring and identifying decentralized transactions conducted by semi-anonymous crypto asset users. As stated in the 2015 report, the absence of a “central location or entity” to “target for investigative purposes”, “weakens countries’ ability to impose effective and dissuasive sanctions”, and “poses a significant challenge to law enforcement in tracking the proceeds of illicit funds being laundered”.⁸⁹

FATF has recommended focusing on crypto asset intermediaries (exchanges) and other “nodes” in decentralized blockchain-based systems rather than targeting individual crypto asset users. These are key institutions whose activities significantly intersect with what FATF defines as the “regulated fiat currency financial system”. By doing so, FATF has shifted the focus of international AML efforts from the state-backed national currencies of the “upper worlds” to the centralized institutions that “send, receive, and store” crypto assets after they have been transferred to the “underground worlds” of the global economy.⁹⁰

FATF has emphasized the need for “coordination mechanisms” with limited enforceability between state and non-state actors. These measures include efforts such as sharing information and data, formulating and adopting “similar AML/CFT practices for similar products and services with comparable risk profiles”, and mutual legal assistance between countries, including either seizing assets or potentially extraditing individuals accused of money laundering offenses. Nonetheless, FATF recommends considering “a range of effective, proportionate, and dissuasive sanctions”, including the complete banning of blockchain-based activities, only if such measures prove insufficient.⁹¹

virtual asset service providers (VASPs). The report also includes updates on emerging risks related to the use of VAs for money laundering, terrorism financing, and the diversity of this financing, as well as developments in the market. FATF's report reveals that while some jurisdictions have made progress in implementing AML/CFT regulations, global implementation remains delayed. A significant number of governments have yet to take crucial steps to regulate the sector and must urgently prioritize the full implementation of the Standards. Since the adoption of the revised R.15/INR.15 in 2019, 130 FATF mutual evaluation and follow-up reports indicate that 75% of jurisdictions are only partially compliant or non-compliant with FATF requirements—a figure unchanged since April 2023 (75% of jurisdictions partially compliant or non-compliant; 73 out of 98)—showing negligible improvement.” (Online, July 9, 2024, accessed July 19, 2024).

⁸⁹ FATF, 2015: 8-11.

⁹⁰ **Petrus C. van Duyne/Klaus von Lampe/Nikos Passas**, (eds.) *Upperworld and Underworld in Cross-Border Crime*, Wolf Legal Publishers, Nijmegen, 2002; FATF, 2015: 6; **Campbell-Verduyn/ Goguen**, p. 76, FATF, 2015: 6.

⁹¹ FATF, 2015: 9-11.

We must express that we find FATF's risk-based approach appropriate. However, this perspective does not imply a ban from FATF's point of view, nor should it turn into a prohibitive mindset for countries aiming to comply with FATF's approach and recommendations on this matter. A risk-based approach is correct, as crypto assets are currently not used as extensively for money laundering as often exaggerated. However, it is a fact that they carry this potential if not controlled. Therefore, FATF has developed a risk-based approach toward this potential scenario. Indeed, this is also expressed in the highly significant and groundbreaking article by *Campbell-Verduyn* on this topic:

*"...despite some shortcomings, the risk-based approach formulated by the Financial Action Task Force (FATF), the leading global organization involved in coordinating anti-money laundering efforts, effectively balances the current threats and opportunities posed by crypto assets. FATF's encouragement of more flexible, decentralized governance networks is considered innovative and, ultimately, more effective than traditional centralized forms of enforcement in an era of rapid and unpredictable technological change."*⁹²

However, we must express that we do not support FATF's extreme approach, which suggests completely banning crypto asset activities if necessary. There are two reasons for this: Firstly, such a ban would hinder technological progress. This would obstruct innovation and efforts to explore ways of achieving a better and more prosperous life. Once such bans begin, they may spread everywhere for various reasons, ultimately impeding the development of science, technology, and humanity. Secondly, a normative ban of this kind would lack practical application in real life, meaning such a prohibitive norm would inevitably fail in terms of social effectiveness. The genie is already out of the bottle! It is no longer possible to prevent the use and development of blockchain and crypto assets through legal rules. Such a ban would push the entire crypto asset sector underground, leading to the commission of far more crimes and complete chaos. Therefore, rather than banning, we believe it would be far more appropriate to work on and implement regulations to bring the sector under control.

The widespread perception that blockchain technology and its applications pose a challenge to the international AML regime has shaped the direction of international organizations' responses. The United Nations Office on Drugs and Crime (UNODC) has prepared a detailed guide for identifying and seizing crypto assets involved in money laundering. In collaboration with the Organization for Security and Co-operation in Europe (OSCE), UNODC has also begun training authorities to investigate money laundering through crypto assets (United Nations Office on Drugs and Crime, 2017). Interpol and Europol have established a partnership to coordinate police activities "against the misuse of virtual currencies for criminal activities and

⁹² *Campbell-Verduyn*, p. 284.

money laundering”.⁹³ Additionally, the European Union has issued directives on this matter. The criticisms we have raised regarding FATF also apply to the regulations implemented by these institutions.

Emerging Risks, Threats, and Challenges

It is an undeniable fact that the use of crypto assets in money laundering and terrorist financing poses a growing threat. This threat has put the financial world on one hand grappling with these challenges and law enforcement on the other hand facing the difficult task of tracing the origins of illicit funds and identifying the criminals involved in generating these illegal funds. The already difficult process of detecting money laundering has become even more challenging with the emergence of crypto assets. Individuals laundering illicit gains are increasingly using crypto assets to clean funds obtained from various criminal activities. Tracking these illegal funds back to their source has become a complex task for law enforcement, as they often rely on traditional investigative methods that are not well-suited to the unique features of crypto assets. Indeed, the use of crypto assets in the stages of money laundering—placement, layering, and integration—has made laundering activities more complex and harder to trace. Criminals leverage crypto asset tumblers and mixing services to obscure the origin of their illicit profits, making it more difficult for law enforcement to follow the money trail and identify the perpetrators.⁹⁴

Among crypto assets, Bitcoin is the first decentralized peer-to-peer (P2P) payment network operated by its users without central governing bodies or intermediaries. From the users’ perspective, Bitcoin is similar to cash but functions exclusively online. The decentralization and anonymity inherent to crypto assets increase the risk of their use for money laundering and terrorist financing. Bitcoin accounts do not contain identity information about account holders, and the system lacks a central server or service provider, which facilitates the execution of laundering activities. The Bitcoin protocol, like real-world cash systems, neither requires nor provides mechanisms for monitoring individuals or generating and maintaining historical transaction data. Additionally, there is no central authority overseeing the system, and currently, there is no complete software capable of monitoring and detecting suspicious transaction patterns to combat money laundering and terrorist financing effectively. As a result, Bitcoin provides a high level of anonymity that is unattainable with credit and debit cards or electronic payment systems (e-wallets). The main issue with crypto assets lies in their very

⁹³ **Campbell-Verduyn/Goguen**, p. 76. see: Europol Interpol Cybercrime Conference makes the case for multisector cooperation. Retrieved 02.10.2015 (Online) <https://www.europol.europa.eu/media-press/newsroom/news/europol-%E2%80%93-interpol-cybercrime-conference-makes-case-for-greater-multisector-cooperation>, (accessed) 10.08.2024

⁹⁴ **Financial Crime Academy**, Crypto Money Laundering.

nature, as they exist entirely outside of established financial institutions and regulatory frameworks.⁹⁵

From a user's perspective, Bitcoin is an electronic money system. Anyone with internet access and sufficient memory capacity on their computer can use this electronic money. The first step to start using Bitcoin is selecting a wallet from the "bitcoin.org" website and setting it up. Once a wallet is created, a Bitcoin address is automatically generated. Using this wallet, the user can perform any transaction. Transferring Bitcoins from one user to another is done by transferring them from one address to another. Since the address appears as a combination of numbers and letters, it provides full anonymity to the owner, e.g., "1D5wZqCjxNuPqfUN3RMFsxxxxtqRBwiAeTZ." Each Bitcoin wallet contains classified information about the private keys of Bitcoin addresses belonging to a specific user. Thus, a transaction can be performed if the private key of a Bitcoin address designed for the transaction is available. Although this system is quite secure, site administrators recommend using as many Bitcoins addresses as possible, ideally creating a new address for each transaction. In the Bitcoin system, there is no feature for recovering a lost private key, so if the private key is lost, the user also loses all funds stored at that address. Similarly, the theft of a private key results in the loss of the Bitcoins stored there. Transaction data is stored in an open-access distributed database without revealing any information about the address owner. To prevent situations where the same Bitcoins are spent twice, *Satoshi Nakamoto* developed a timestamp server that divides the database into unique blocks in a blockchain. Each block contains the hash (checksum) and serial number of the previous block. A new block is created when transactions are confirmed, and it includes information about prior Bitcoin transactions. In other words, each Bitcoin contains a history of how it was previously used. When users transfer Bitcoins, they leave a "digital signature" and the public key of the next owner. If data within a block is altered, the HASH value changes, causing other blocks to reject this different HASH value. As a result, data cannot be tampered with.⁹⁶ All transactions are linked to Bitcoin addresses, and their traces can be followed on the Bitcoin blockchain available online. Therefore, the information on Bitcoin addresses found on a suspect's computer can be examined to determine which transactions occurred before and after transfers to Bitcoin addresses linked to the suspect.⁹⁷

The effects of technology on global governance have often given rise to two contradictory perspectives. On one side, there are optimistic views based on the belief

⁹⁵ **Diana Mergenovna Sat/Grigory Olegovich Krylov/Kirill Evgenyevich Bezverbnyi/Alexander Borisovich Kasatkin/Ivan Aleksandrovich Kornev**, "Investigation of Money Laundering Methods Through Cryptocurrency", *Journal of Theoretical and Applied Information Technology*, Vol. 83, No. 2, January 2016, p. 245

⁹⁶ **Akbulut**, p. 490.

⁹⁷ **Sat/Krylov/Bezverbnyi/Kasatkin/Kornev**, pp. 245, 246.

that advancements in technology will enhance governance;⁹⁸ on the other, there are pessimistic perspectives embedded in dystopian narratives that suggest new technologies will have negative consequences for governance.⁹⁹ The first view assumes that technological advancements will lead to increased economic efficiency and improved human living conditions. The second focuses more on the catastrophes caused by technological progress, such as nuclear weapons or toxic particles, and the looming risks of extinction. Both perspectives oversimplify the far more complex and intertwined relationship between technology and governance.¹⁰⁰ In reality, things do not progress as straightforwardly in a positive direction, nor do they entirely decline in a negative way. Technology is deeply embedded in the power structures of daily life and is in a constant state of evolution. Moving beyond the “two narratives” of technology pushes us to look past superficial instrumentality and focus on the deeper relationships between technology and governments, businesses, individuals, and other entities.¹⁰¹

The emergence of Bitcoin and blockchain technology exemplifies these power dynamics. On one hand, disintermediation, which enables individuals to transact directly without central institutions, empowers people against the control of governments or central banks. On the other hand, central institutions are not entirely sidelined by this technology. Instead, governmental policy responses specifically targeting cryptocurrencies and, more broadly, blockchain technology, play a significant role in shaping their developmental trajectory.¹⁰²

In a study focused on Bitcoin, *van Wegberg, Oerlemans, and van Deventer* concluded that laundering proceeds of crime through cryptocurrency is a concept that is feasible in practice. They found that laundering via cryptocurrencies today shares significant similarities with traditional methods of money laundering, making it highly adaptable to future laundering practices. The authors highlight that recent cases and Europol reports provide evidence supporting the use of Bitcoin by cybercriminals for laundering purposes. What the authors consider most noteworthy is that laundering through cryptocurrencies offers greater anonymity while reducing the costs of laundering, making this method more appealing to criminals as a money-laundering technique. They pose the question of what this means for the profitability of crime models. In addressing this question, they acknowledge the limited scope of their

⁹⁸ **Ray Kurzweil**, *The Singularity is Near: When Humans Transcend Biology*, Penguin, London, 2005; **Roger Pielke Jr./Tom Wigley/Christopher Green**, *Dangerous Assumptions Nature*, 452, 2008, pp. 531–532.

⁹⁹ **Steve Matthewman**, *Technology and Social Theory*, Palgrave Macmillan, London, 2011.

¹⁰⁰ **Maximilian Mayer/Mariana Carpes/Ruth Knoblich**, (eds.), *The Global Politics of Science and Technology – Vol. 1, Concepts from International Relations and Other Disciplines*, Springer, New York, 2014; **Maximilian Mayer/Mariana Carpes/Ruth Knoblich**, (eds.), *The Global Politics of Science and Technology – Vol. 2, Perspectives, Cases and Methods*, Springer, New York, 2014.

¹⁰¹ **Kai Jia/Falin Zihang**, “Between Liberalization and Prohibition Prudent Enthusiasm and the Governance of Bitcoin/blockchain Technology”, in: *Bitcoin and Beyond Cryptocurrencies, Blockchains, and Global Governance*, Ed. Malcolm Campbell-Verduyn, Routledge, London and New York, 2018, p. 88.

¹⁰² **Jia/Zihang**, p. 89.

understanding of criminals using this method. However, based on their small-scale experiment, they assert that, at least in theory, laundering with Bitcoin can reduce costs, potentially making certain crime models more profitable, thereby increasing their attractiveness for cybercriminal enterprises.¹⁰³

Crypto assets are used for both good and evil. Among jurisdictions, the two most common illegal uses of crypto assets are digital black markets (illegal marketplaces) and the laundering of proceeds of crime. Transferring proceeds of crime beyond the physical borders of countries through the anonymity provided by the internet, a global network, has become significantly easier thanks to this technology. From a theoretical perspective, it might be thought that crypto assets are not as attractive an option for those who want to launder proceeds of crime as they might appear. Firstly, the scope of transactions involving crypto assets is limited. Secondly, all transaction records are public and accessible. Although users' addresses and identities are protected by encryption technology, as seen particularly in the Silk Road case, when Bitcoins are exchanged for certain fiat currencies, it is still possible for law enforcement to identify suspects. Thirdly, as observed in the European Union, legal regulations are gradually being introduced to Bitcoin exchanges, which are under pressure to comply with anti-laundering record-keeping and reporting requirements.¹⁰⁴ However, these concerns do not eliminate the potential suitability of crypto assets for laundering purposes. Some of the challenges faced by law enforcement in combating the use of crypto assets for laundering include the following: The first challenge is the decentralized nature of crypto assets. Unlike traditional currencies, crypto assets are not controlled by any central authority and allow transactions to occur outside the oversight of governments or financial institutions.¹⁰⁵ This decentralized and distributed structure significantly complicates law enforcement's efforts to trace and monitor illicit funds. Additionally, the lack of a global regulatory framework further complicates criminal investigations. Moreover, the pseudonymous and anonymous nature of crypto asset transactions adds another layer of complexity. While all transactions are recorded on the blockchain, asset transfers are made using cryptographic addresses, which makes it difficult to associate transactions with the real-world identities of those conducting them. This provides a level of anonymity that can be exploited by criminals, hindering the efforts of law enforcement. The execution of transactions without the need for intermediaries, such as banks, and the cross-border nature of crypto assets with global accessibility pose yet another challenge for law enforcement in tracking criminals. In this way,

¹⁰³ van Wegberg/Oerlemans/van Deventer, p. 431.

¹⁰⁴ Aaron van Wirdum, "New EU directive may impose anti-money laundering regulations on Bitcoin wallet providers", Bitcoin Magazine, (2016), (Online) <https://bitcoinmagazine.com/articles/new-eudirective-may-impose-anti-money-laundering-regulations-on-bitcoin-wallet-providers-1468424029/> (accessed) 09.08.2024; Jia/Zihang, pp. 95, 96.

¹⁰⁵ Çakır, p. 78; Akbulut, p. 489.

proceeds of crime in one country can be easily transferred to another, making the identification and investigation of criminals significantly more difficult.¹⁰⁶

Another challenge in this field is that some crypto assets provide additional privacy. The most notable examples are privacy altcoins such as Monero and Zcash. These crypto assets, referred to as privacy coins, are specifically designed to mask a user's information and details related to a transaction. While these assets are public in the sense that they have public ledgers, transaction details are concealed to varying degrees to protect the privacy of end users. As a result, privacy assets like Monero and Zcash provide an additional layer of anonymity that may benefit criminals while simultaneously hindering law enforcement investigations. Privacy assets can also circumvent the software/tools developed to track crypto assets, making their existence a factor that increases risk.¹⁰⁷ Among these, Monero makes it difficult to trace the parties involved in a transaction because transaction signatures are shared among a large group of people, making it highly challenging to associate specific users with a transaction. Zcash, on the other hand, operates somewhat differently, providing privacy by "erasing" transaction history after the transaction has been completed.¹⁰⁸ For this reason, considering the dynamic nature of the industry and the lack of visibility into the proprietary technologies developed (or to be developed) by operators in this field, there is ongoing debate over whether a general ban would be the most appropriate course of action moving forward.¹⁰⁹

Although privacy crypto assets may appear highly suitable for those laundering proceeds of crime, it should be noted that these assets were not developed with the intent of manipulating 21st-century technology to modernize an age-old crime. Instead, privacy assets are designed to provide individuals with an additional layer of privacy, security, and anonymity in the digital age. In fact, Monero was developed for most people to use legally, with the aim of ensuring privacy for individuals who simply do not want others to know whether they are buying coffee or a car.¹¹⁰ However, as with most technological advancements, inventors may have good intentions, but some individuals will always find ways to misuse the technology for malicious purposes. Nevertheless, privacy assets like Monero and Zcash, due to their potential for misuse,

¹⁰⁶ **Financial Crime Academy**, Crypto Money Laundering.

¹⁰⁷ **Buttigieg/Efthymiopoulos/Attard/Cuyle**, p. 214.

¹⁰⁸ **Forgang**, p. 7. See also Nasdaq, "Know Your Coins: Public vs. Private Cryptocurrencies," September 22, 2017, (Online) <https://www.nasdaq.com/articles/know-your-coins-public-vs-private-cryptocurrencies-2017-09-22>, (accessed) July 10, 2024.

¹⁰⁹ **Buttigieg/Efthymiopoulos/Attard/Cuyle**, p. 214.

¹¹⁰ **Olga Kharif**, "Bitcoin is being dropped by criminals in favour of privacy coins like monero", Independent, January 2 2018, (Online) <https://www.independent.co.uk/news/business/analysisand-features/bitcoin-latestupdates-price-privacy-coins-cryptocurrency-monero-digital-currencypricea8137901.html>, (Accessed) 10.07.2024

have garnered significant attention from both law enforcement agencies and international regulators.¹¹¹

In conclusion, *Keech*, representing the general opinion of those working in this field, emphasizes the need to strike a balance between the existing threats and the opportunities provided by crypto assets.¹¹² Similarly, *Campbell-Verduyn* acknowledges that steps to prevent the laundering of proceeds of crime should shift focus from the illegal use of crypto assets to the blockchain technology underlying cryptocurrencies.¹¹³

Measures to Be Taken

1. In General

Crypto assets have revolutionized the financial world by offering new opportunities for innovation and investment. Alongside the benefits of this digital revolution, a darker side has also emerged. On the darker side, crypto assets are being used in the commission of various crimes and in laundering proceeds of crime. As criminals develop increasingly sophisticated methods to exploit the anonymity and decentralized nature of crypto assets, it is essential for law enforcement, policymakers, and the crypto industry to work together to combat this growing threat.

The global nature of crypto assets necessitates a coordinated international intervention and collective effort to effectively combat crypto asset laundering. Criminals aiming to make their activities more complex continually refine their techniques to stay ahead of investigative authorities. The rapid advancements in technology, combined with limited resources and expertise, make it challenging for authorities to keep pace with the ever-evolving crypto asset laundering landscape. As a result, law enforcement must adapt and develop new strategies to effectively counter this growing threat.¹¹⁴

Criminals continuously refine their crime commission and money laundering techniques, both through traditional methods and by leveraging crypto assets and the digital world. This constant evolution makes it increasingly difficult for law enforcement to effectively combat the laundering of proceeds of crime and keep up with technological advancements. Understanding the techniques used by criminals is a crucial step in effectively fighting crypto money laundering. Law enforcement and

¹¹¹ **Shaurya Malwa**, "\$1.2 Billion in Cryptocurrency Laundered Through Bitcoin Tumblers, Privacy Coins," July 6, 2018, (Online) <https://finance.yahoo.com/news/1-2-billion-cryptocurrency-laundered-224521652.html>, (accessed) July 11, 2024; **Forgang**, p. 8.

¹¹² **Keech**, p. 57.

¹¹³ **Campbell-Verduyn**, p. 283

¹¹⁴ **Financial Crime Academy**, Crypto Money Laundering.

regulatory bodies must uncover these techniques and develop strategies and tools to counter laundering activities and maintain the credibility of the crypto industry.¹¹⁵

2. The Role of Crypto Asset Intermediaries (Exchanges) in Combating Money Laundering

Crypto asset intermediaries, also known as crypto asset exchanges, occupy a critical position in the initial stage of combating the laundering of proceeds of crime. As a significant component of the crypto ecosystem, these institutions must be assigned various obligations not only to ensure the proper functioning of the ecosystem but also to combat the laundering of proceeds of crime and the financing of terrorism. These institutions should be required to implement strict KYC (Know Your Customer) and AML (Anti-Money Laundering) policies, detect and report suspicious activities, and cooperate with investigative authorities.¹¹⁶ Indeed, in Türkiye, MASAK (Financial Crimes Investigation Board) has recently introduced these obligations for crypto asset intermediaries.

Crypto assets are not issued by traditional financial institutions and, therefore, are not subject to the same regulations. While individuals can freely exchange crypto assets without the need for a financial intermediary, crypto asset intermediaries can also be exploited to facilitate money laundering activities. Essentially, intermediaries are trading platforms where crypto assets can be legally bought and sold, allowing for the conversion of traditional currencies into crypto asset units, the reverse process, and the exchange of one crypto asset unit for another. Although some intermediaries have protocols in place to prevent money laundering, it should be noted that vulnerabilities that can be exploited still exist. After all, even the largest and most heavily regulated financial institutions are not entirely immune to money laundering activities. The fact that these institutions have compliance departments and employ anti-money laundering officers does not mean that money laundering activities no longer occur.¹¹⁷

Among these institutions, a distinction can be made between those that comply with KYC/AML regulations and those that do not. Compliant intermediaries are institutions that adhere to the laws and regulations related to KYC/AML obligations and conduct their operations accordingly. Through this compliance, intermediaries assist investigative authorities in preventing money laundering and other illegal activities while also protecting their users from potential risks. These institutions must take their responsibilities seriously by ensuring they have robust systems and procedures in place to verify their users' identities, monitor transactions for signs of suspicious activity, and report potential issues to the relevant authorities. Not only does this help maintain the integrity of the crypto ecosystem, but it also demonstrates their commitment to

¹¹⁵ **Financial Crime Academy**, Crypto Money Laundering.

¹¹⁶ **Financial Crime Academy**, Crypto Money Laundering.

¹¹⁷ **Forgang**, p. 7.

operating transparently and ethically, thereby building trust among their users and the broader public. In contrast, non-compliant exchanges do not implement strict KYC/AML policies, making them more vulnerable to criminal activities and potential shutdowns by authorities. The distinction between compliant and non-compliant exchanges highlights the importance of regulation and oversight in the crypto sector. Regulators should ensure that exchanges adhere to strict KYC/AML requirements to help prevent money laundering and other illegal activities while also preserving the integrity of the crypto ecosystem. This, in turn, fosters greater trust among users, investors, and other stakeholders in the sector.¹¹⁸

Detecting and tracking the use of blockchain applications in criminal activities entails various challenges. The response to these challenges has been the implementation of decentralized and flexible international rules (soft law principles). In other words, states and non-state actors have promoted the development of various AML-compliant activities to address these difficulties. On one hand, judicial authorities in different parts of the world have sought to distinguish themselves as legitimate hubs for AML-compliant blockchain activities. For instance, in the United States, New York State has developed a “Bitlicense” granted to intermediary institutions that fulfill commitments such as “annual risk assessments, maintaining ten-year records of all transactions, suspicious activity reports, customer identification programs, controls and compliance, annual internal or external audits, and refraining from structuring activities to avoid reporting or conceal identities.” Similarly, rival regions such as Singapore have worked to attract AML-compliant blockchain-based activities. In Singapore, the Suspicious Transaction Reporting Office actively verifies user identities and monitors suspicious transactions. The Channel Island of Alderney promotes itself as an AML-compliant blockchain hub and competes with the Isle of Man for the title of “Bitcoin Island”. In a similar vein, it is stated that some crypto asset intermediaries have voluntarily accepted and declared their compliance with the KYC/AML regime.¹¹⁹

In recent years, crypto asset intermediaries have undergone significant changes in adopting KYC/AML practices. In the past, it was possible to sign up for an account and deposit or withdraw funds on exchanges with minimal or no information beyond an email address. However, as intermediaries have now grown into large and profitable businesses, implementing due diligence and aligning with similar financial institutions has become a more logical step for these organizations. There remains a perception that the crypto asset sector is unregulated and that crypto assets are still associated with illegal activities due to their early use on platforms like Silk Road and the dark web. As the sector expands, self-regulation and regular reporting will be steps in the right direction, particularly as large financial institutions invest, and crypto assets establish themselves within the financial industry. Centralized exchanges have transformed into platforms operating in KYC/AML-friendly jurisdictions with high AML regulatory

¹¹⁸ **Financial Crime Academy**, *Crypto Money Laundering*.

¹¹⁹ **Campbell-Verduyn/Goguen**, p. 78.

standards. Exchanges operating in these regions are aware that failing to meet the expected standards increases the likelihood of stringent regulatory action. Poorly managed intermediaries expose their customers to risks. These exchanges attract an immense number of customers and generate substantial profits, as demonstrated by Binance, a relatively new exchange, which declared higher earnings (over \$200 million) than Germany's largest bank within the same period.¹²⁰ Therefore, compliance with KYC/AML regulations is crucial for the credibility of crypto asset intermediaries, their capacity to attract customers, and, consequently, their profitability.

As the first line of defense against the laundering of proceeds of crime, crypto asset service providers must take robust measures to protect their businesses and customers from financial crimes. The first of these measures is the implementation of strong KYC and AML policies. For crypto asset intermediaries seeking to mitigate laundering risks, implementing robust KYC and AML policies is a critical step. By accurately identifying and verifying their customers and assessing their risk profiles, these institutions can ensure they do not unintentionally facilitate laundering activities or provide services to individuals involved in criminal activities. Strong KYC/AML policies not only protect intermediaries from various administrative sanctions but also demonstrate a commitment to complying with regulations aimed at preventing the laundering of proceeds of crime. This commitment helps build trust among customers, investors, and other stakeholders.¹²¹

The second measure is the implementation of employee training and awareness programs. These programs are an essential component of a comprehensive anti-money laundering strategy. Crypto asset intermediaries can reduce the likelihood of their services being used for illegal purposes by ensuring that their employees are well-informed about money laundering risks and equipped to identify warning signs. This approach enhances the institution's ability to proactively address and mitigate financial crime risks.¹²²

Another measure is the proactive monitoring and reporting of suspicious activities. Proactively monitoring and reporting suspicious activities is a crucial part of an effective anti-money laundering strategy. By closely monitoring transactions and identifying unusual patterns or behaviors, crypto asset institutions can detect potential laundering schemes and take appropriate measures to prevent them from being carried out.¹²³

In this context, the key players in the crypto asset space include crypto asset users, issuers/managers of crypto assets, crypto asset exchanges, wallet providers, trading

¹²⁰ Dyson/Buchanan/Bell, p. 3.

¹²¹ Financial Crime Academy, Crypto Money Laundering

¹²² Financial Crime Academy, Crypto Money Laundering.

¹²³ Financial Crime Academy, Crypto Money Laundering.

platforms, and crypto mining pools. To adequately mitigate the AML/CTF risks associated with crypto assets, it is vital to begin regulating specific key players involved in crypto asset transactions. These players should be subject to AML/CFT requirements, including implementing KYC procedures, monitoring transactions, and issuing Suspicious Transaction Reports to flag high-risk transactions, just as is done for traditional financial instruments.¹²⁴

Crypto asset intermediaries should closely examine transactions for signs of suspicious activity, identify potential laundering operations, and take appropriate measures to prevent them. Intermediaries must comply with their obligations to report suspicious transactions to the relevant authorities and freeze the associated assets. These institutions should also invest in advanced tools and technologies to monitor transactions effectively and detect warning signs, as well as achieve the necessary expertise to analyze and interpret complex transaction data. Furthermore, intermediaries should collaborate with law enforcement agencies and other stakeholders in the crypto sector to share information and resources. This cooperation will make it easier to detect and prevent laundering activities, including tracing and halting the laundering of funds.¹²⁵

In this context, monitoring fund transactions involving crypto assets and identifying suspicious transaction alerts (red flags) are essential components of an effective anti-money laundering strategy. Developing typologies for combating proceeds of crime involving crypto assets will aid in creating red flags that indicate suspicious and high-risk crypto transactions, thereby supporting effective and efficient AML/CFT compliance.¹²⁶

Collaboration between crypto asset intermediaries and law enforcement is crucial for the effective investigation and prosecution of crypto asset laundering cases. By working together, intermediaries can provide valuable information and support to law enforcement while also benefiting from the expertise and resources of these authorities. In addition to sharing information and resources, cooperation between crypto asset intermediaries and law enforcement can help shape policies and regulations that promote transparency and safeguard against illegal activities. By collaborating, both parties can better understand the risks and challenges associated with crypto asset laundering and develop strategies and tools to combat this growing threat.¹²⁷

3. Investigative Tools and Techniques for Identifying Proceeds of Crime

¹²⁴ Buttigieg/Efthymiopoulos/Attard/Cuyle, p. 214.

¹²⁵ Financial Crime Academy, Crypto Money Laundering.

¹²⁶ Buttigieg/Efthymiopoulos/Attard/Cuyle, p. 214.

¹²⁷ Financial Crime Academy, Crypto Money Laundering.

Law enforcement agencies must have access to cutting-edge tools and techniques to effectively combat laundering operations conducted through crypto assets, trace proceeds of crime, and identify perpetrators. Given the unique nature of crypto assets, their decentralized structure, and the anonymity they can provide to users, this need is particularly critical. Traditional methods for tracing and tracking proceeds of crime are often inadequate in the face of these challenges, necessitating the development and adoption of advanced investigative techniques specifically tailored to the field of crypto assets.¹²⁸

These tools and techniques must be capable of identifying suspicious transaction patterns, detecting potential illegal activities, and even predicting future threats by analyzing complex blockchain data. Additionally, due to the anonymous nature of crypto asset transactions, they should provide mechanisms to link blockchain transactions to real-world identities, a process that is often complex. These tools need to be dynamic and adaptable to keep pace with the rapid evolution of crypto technologies and laundering methods. As criminals continue to innovate and adopt new strategies to exploit crypto systems, law enforcement must ensure that investigative tools and techniques are not only up-to-date but also forward-looking, capable of anticipating and countering emerging threats.¹²⁹ This is especially critical when crypto asset intermediaries have inadequate KYC protocols for onboarding new clients. If intermediaries fail to maintain sufficient records about their customers or make reasonable efforts to verify the information, law enforcement may lack the necessary resources to investigate suspicious activities.¹³⁰ As noted in an article from The Wall Street Journal, *“tech-savvy criminals are increasingly opening accounts under false names on overseas exchanges that do not comply with U.S. laws”*. Moreover, according to a former U.S. prosecutor from the Department of Justice, *“While investigators can analyze blockchain to trace funds, they may not be able to link those funds to a real-world criminal. Subpoenas might return a name like ‘Mickey Mouse’ residing at ‘123 Main Street.’”*¹³¹

In addition to these advanced tools and techniques, law enforcement must have access to comprehensive and timely information. Achieving this requires close collaboration with crypto asset intermediaries, financial institutions, regulatory bodies, and other relevant stakeholders. Through information sharing and joint efforts, a more transparent and secure crypto environment can be created, making it significantly more

¹²⁸ **Financial Crime Academy**, Crypto Money Laundering.

¹²⁹ **Financial Crime Academy**, Crypto Money Laundering.

¹³⁰ **Forgang**, p. 13

¹³¹ **Corinne Ramey**, “The Crypto Crime Wave is Here: From stickups and drug deals to white-collar scams, cryptocurrency-related crime is soaring—and law enforcement is scrambling to keep up”, The Wall Street Journal, April 26 2018, (Online) <https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366>, (accessed) 11.07.2024.

challenging for criminals to exploit the system for laundering proceeds of crime and engaging in other illegal activities.¹³²

Money laundering operations involving crypto assets often start and end with the exchange of currencies. Law enforcement can collect evidence during these exchanges. Since existing policing measures provide sufficient tools for this purpose, there is a possibility of effective intervention. To track crypto asset transfers, law enforcement must identify the addresses associated with these assets and seize and analyze the crypto asset wallets of identified offenders. This approach can help uncover illicit activities and provide critical evidence in investigations.¹³³

Blockchain analysis and digital forensics can play a critical role in helping law enforcement trace and recover proceeds of crime. By examining blockchain data, investigators can identify suspicious transactions and patterns, and even pinpoint individuals involved in criminal activities. This is valuable not only for cases of cryptocurrency laundering but also for investigating and prosecuting other types of financial crimes. However, blockchain analysis and digital forensics face several challenges, including the complexity of blockchain technology, the lack of standardized data, and the shortage of expertise. To overcome these challenges, law enforcement agencies must invest in the necessary tools and training and collaborate closely with the crypto industry to share knowledge and resources.¹³⁴

Blockchain-based initiatives can leverage big data analysis to create profiles of crypto asset users by identifying individuals associated with specific crypto asset addresses. Since the Bitcoin network inherently publishes the history of all transactions conducted so far, analyzing this data can reveal insightful information about specific nodes and their transactional activities. Companies such as BlockTrail and Coinanalytics enhance the ability of intergovernmental police organizations, like Europol and Interpol, to match crypto asset transactions with individual profiles by identifying specific usage patterns. Transaction flows are linked to identities associated with certain users through forensic tools for crypto assets developed by computer scientists. These and other initiatives demonstrate that blockchain technologies can “function” to contribute to global AML governance efforts in terms of information and identity identification, rather than undermining them. Furthermore, they broadly exemplify how new technologies can not only challenge regulatory efforts but also support them. Thus, the paradox of blockchain technology lies in the fact that while AML efforts must contend with the “imperfect knowledge of identities”, they can also benefit from the “perfect knowledge of all transactions”.¹³⁵

¹³² **Financial Crime Academy**, Crypto Money Laundering

¹³³ **van Wegberg/Oerlemans/van Deventer**, p. 431.

¹³⁴ **Financial Crime Academy**, Crypto Money Laundering.

¹³⁵ **Campbell-Verduyn**, p. 298.

The primary innovation of Distributed Ledger Technology (DLT) lies in its cryptographic protection and the ability to share an ever-updating record with multiple parties. Distributed networks like blockchains offer a shared database that transparently and securely records all network activities. Since the history of crypto asset transactions is logged in the ledger, this record is immutable (unless a 51% attack on the entire system occurs, which is nearly impossible) and results in permanent records. This allows for the collection of significant amounts of data from public ledgers, as every transaction address can be searched on the respective DLT, such as the Bitcoin blockchain. The information on the distributed ledger can subsequently be used to link crypto asset addresses to the digital identities of their owners and investigate the source, activity, and destination of crypto funds, but only if DLT analysis software is available. DLT analysis software enables the attribution of addresses to specific users and provides comprehensive reports on the source of funds. It assists in creating controls and risk assessments for AML/CFT and KYC requirements while also supporting the investigation of other economic crimes. The application of this technology plays a crucial role in developing money laundering typologies and establishing a pool of red flag indicators, aiding prevention, oversight, and forensic investigations in the field of crypto assets.¹³⁶

Crypto assets, in addition to facilitating illegal trade, also make it easier to detect illegal activities due to the public nature of blockchain technology. Despite Bitcoin's widespread use in illegal activities, some authors argue that, although crypto assets have an anonymous structure, blockchain actually facilitates law enforcement's detection of illegal activities. These authors have demonstrated that they can link individual transactions to the IP addresses of senders by tracing transactions uploaded from computers to the blockchain.¹³⁷ Other researchers explain how a Bitcoin theft on the blockchain can be traced back to Bitcoin exchanges and how this method can potentially be used to identify perpetrators.¹³⁸ Another author suggests that the growing popularity of Bitcoin will inevitably lead to a growing market for anonymization

¹³⁶ Buttigieg/Efthymiopoulos/Attard/Cuyle, p. 215

¹³⁷ Philip Koshy, Diana Koshy, and Patrick McDaniel, in their article "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic," published in the 18th International Conference on Financial Cryptography and Data Security, edited by Reihaneh Safavi-Naini and Nicolas Christin (Springer Verlag, Heidelberg, 2014, pp. 469–485), included the following statement in the abstract of their article:

"Over the past four years, Bitcoin, a decentralized P2P cryptocurrency, has garnered widespread attention. The ability to create supposedly anonymous financial transactions using Bitcoin has made the currency appealing to privacy-conscious users. While previous studies have analyzed the degree of anonymity offered by Bitcoin using clustering and flow analysis, none have demonstrated the ability to directly match Bitcoin addresses with IP data. We propose a novel approach to establish and evaluate such matches using real-time transaction traffic collected over just five months. We developed heuristic methods to identify ownership relationships between Bitcoin addresses and IP addresses. We discuss the conditions under which these relationships become evident and demonstrate how approximately 1,000 Bitcoin addresses can be matched with their likely owner IPs by exploiting abnormal transmission behavior."

¹³⁸ Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage, pp. 86-93.

technologies, which, in turn, will increase the transparency of users conducting transactions on the blockchain.¹³⁹

Despite the use of advanced and obfuscating crypto strategies, powerful intelligence toolkits have been developed to help uncover the anonymity of crypto asset transactions through complex data analytics. These toolkits are the result of automated DLT analysis software solutions developed by forensic technology companies such as Regtech. By tracking complex illegal transactions, blockchain analysis solutions can assist with AML/CFT and KYC compliance obligations. They publish activity monitoring reports, help visualize and investigate the origins and destinations of suspicious transactions and detect suspicious activities and emerging threats from the dark web. In this way, crypto asset transactions can be traced and linked to an individual's public key address.¹⁴⁰ In response to these developments, advocates of the anonymity provided by crypto assets are developing new currencies that challenge law enforcement detection methods. Among these are Monero,¹⁴¹ which hides a user's public key among a group of public keys containing the same amount (known as "ring signatures"),¹⁴² and Zcash,¹⁴³ which leaves no trace by concealing the sender, receiver, and transaction amount. Notably, the "Z" in Zcash derives from the word "zero", signifying zero knowledge and the absence of information disclosure.¹⁴⁴

¹³⁹ Yermack, pp. 7–31.

¹⁴⁰ Buttigieg/Efthymiopoulos/Attard/Cuyle, p. 215

¹⁴¹ For detailed information, see. **Shen Noether**, "Ring Signature Confidential Transactions for Monero". IACR Cryptology ePrint Archive, 2015, (Online) <https://eprint.iacr.org/2015/1098>, (accessed) 16.07.2024.

¹⁴² Ring signature provides data confidentiality and user identity privacy. Ring signature is a type of cryptographic digital signature based on a group of users (referred to as a ring) provided with asymmetric keys for signing messages. Once a message is signed, it can only be decrypted with the ring signature, and the true signer of the message within the group cannot be identified. As an example of application, the Ring CryptoNote protocol conceals transaction details (e.g., amount, source, destination) in the decentralized cryptocurrency Monero. However, ring signatures require a TTP (Trusted Third Party) to manage user identities, and due to digital certificates, both the generation and verification cost of ring signatures increases. Identity-based ring signatures overcome these issues and enhance user privacy. They also provide protection against full key exposure attacks." See. **Sidra Aslam/Aleksandar Tošić/Michael Mrissa**, "Secure and Privacy-Aware Blockchain Design: Requirements, Challenges and Solutions," *Journal of Cybersecurity and Privacy*, Vol. 1, 2021, p. 171.

¹⁴³ For detailed information, see. **Eli Ben Sasson/Alessandro Chiesa/Christina Garman/Matthew Green/Ian Miers/Eran Tromer/Madars Virza**, "Zerocash: Decentralized Anonymous Payments from Bitcoin," *IEEE Symposium on Security and Privacy*, 2014, (Online) <https://ieeexplore.ieee.org/document/6956581>, (accessed: July 16, 2024).

"This crypto asset derives its name directly from the concept of 'zero-knowledge proof' (ZKP). Zero-knowledge proof (ZKP) allows one entity (the prover) to demonstrate to another entity (the verifier) that a specific value is true without providing any information other than the correctness of the proof itself. Zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) are a type of ZKP that enables the prover to demonstrate the correctness of information to the verifier without any interaction between the two parties. ZKP-based solutions are particularly appealing for data integrity and authentication because they provide proof of a statement without revealing the statement itself. They also preserve anonymity for sensitive data and do not rely on a TTP. However, compared to other solutions, they are computationally intensive for both generating and verifying proofs." See. **Aslam/Tošić/Mrissa**, p. 171; **van Wegberg/Oerlemans/van Deventer**, pp. 423, 424.

¹⁴⁴ **Foley/Karlsen/Putnins**, pp. 8-9

In their article, *Foley, Karlsen, and Putnins* describe techniques they believe could assist law enforcement. According to their findings, it is possible to develop new approaches to identifying illegal activities in Bitcoin by utilizing network clustering analysis and detection-controlled prediction techniques, and these methods can be employed in surveillance activities by law enforcement. For example, these methods can be applied to blockchain data as new blocks are created, enabling authorities to monitor illegal activities in Bitcoin. Such information could help make better use of the currently very limited regulatory and enforcement resources. During their research, a range of crypto assets, known as “privacy coins”, such as Monero, Dash, and Zcash, emerged and were adopted to some extent among illegal users. For instance, some darknet marketplaces began accepting Monero for payments, which, according to the authors, likely reduced the volume of illegal activity in Bitcoin. While the authors note that further development of privacy coins will make detecting illegal activities more challenging, they also point out that, to date, the major privacy coins have failed to provide complete privacy to their users. Computer science researchers have been able to reconstruct user-level records and transaction activities on popular privacy coins like Monero and Zcash using various heuristic methods and clustering algorithms. Based on such findings, it appears that privacy coins may not deliver the level of privacy they aim to provide. As a result, the authors argue that, even if illegal activities continue to shift to popular privacy coins like Monero and Zcash, law enforcement and researchers can use their approaches to investigate crimes committed with privacy coins as well as non-privacy coins like Bitcoin Cash, Litecoin, and Ethereum.¹⁴⁵

In addition to blockchain analysis, financial investigations and traditional techniques can also be employed to uncover money laundering schemes involving proceeds of crime and identify those responsible for such activities. By analyzing financial records, tracing transactions, and interviewing suspects, investigators can piece together the complex network of transactions underlying money laundering schemes and bring offenders to justice. However, relying solely on financial investigations and traditional techniques may not be sufficient to overcome the challenges posed by laundering through crypto assets. To effectively combat this threat, law enforcement must adopt new tools and technologies. Examples of such techniques include blockchain analysis, machine learning algorithms, data analytics, and artificial intelligence software. Moreover, collaborating with the crypto industry to develop innovative solutions for preventing and detecting laundering through crypto assets, as well as sharing knowledge and resources, is crucial.¹⁴⁶

Collaboration with crypto sector stakeholders, such as crypto asset service providers, wallet providers, and other service providers, is crucial for the effective investigation and prosecution of money laundering cases involving crypto assets. By working together, law enforcement and the crypto industry can pool their resources and

¹⁴⁵ **Foley/Karlsen/Putnins**, pp. 33-34.

¹⁴⁶ **Financial Crime Academy**, Crypto Money Laundering.

expertise to detect and prevent laundering activities and ensure that those responsible are brought to justice. In addition to sharing knowledge and resources, cooperation between law enforcement and the crypto industry can contribute to the development of new tools and techniques for tracing illicit funds and combating the laundering of proceeds of crime. This collaboration can help ensure that the crypto ecosystem remains transparent, secure, and free from criminal activities.¹⁴⁷

In conclusion, the laundering of crypto assets poses a significant threat to the financial world and can only be effectively combated through the joint efforts of law enforcement, regulators, and the crypto industry. By implementing robust KYC/AML policies, monitoring transactions for suspicious activities, and collaborating to share knowledge and resources, the crypto ecosystem can be kept transparent, secure, and free from criminal activities. As the world of crypto assets continues to evolve, it is crucial to remain vigilant and proactive in efforts to prevent the laundering of proceeds of crime and to protect the integrity of the financial system.¹⁴⁸

Regulation in Türkiye

Since the topic of this article is the use of crypto assets in the laundering of proceeds of crime, we will not delve further into details, as this regulation is broad and significant enough to constitute the subject of another article. However, we have chosen to provide brief information to demonstrate that Türkiye's legislators have not remained indifferent to the development of crypto assets.

As mentioned in the introduction, in Türkiye, crypto assets and crypto asset intermediary institutions have been regulated through the amendments made to the Capital Markets Law No. 6362, dated 06.12.2012, under Law No. 7518, dated 26.06.2024.

With the additions to Article 3 of the Capital Markets Law (SPK), concepts related to the crypto asset sector, such as *“wallet, crypto asset, crypto asset service provider, crypto asset custody service, and platform”*, have been defined. Accordingly, a wallet is defined as *“software, hardware, systems, or applications that enable the transfer of crypto assets and the online or offline storage of these assets or the private and public keys related to them”*; a crypto asset as *“intangible assets that can be electronically created and stored using distributed ledger technology or similar technology, distributed over digital networks, and that represent value or rights”*; a crypto asset service provider as *“platforms, entities providing crypto asset custody services, and other entities designated to provide services related to crypto assets, including their initial sale or distribution, as determined by regulations made pursuant to this Law”*; a crypto asset custody service as *“the storage, management, or other custody services determined by the Board for crypto assets of platform clients or the private keys*

¹⁴⁷ Financial Crime Academy, Crypto Money Laundering.

¹⁴⁸ Financial Crime Academy, Crypto Money Laundering.

providing transfer rights to these assets from wallets”; and a platform as “entities where one or more of the following transactions are carried out: the purchase and sale, initial sale or distribution, exchange, transfer of crypto assets, and the required custody or other operations to be determined”. Thus, the fundamental aspects of crypto assets have been defined in our legal system in harmony with the established body of knowledge on this subject.

Apart from these definitions, with the addition of Article 35/B to the Capital Markets Law (SPK), the conditions for establishing and operating crypto asset intermediary institutions have been strictly regulated. It has been stated that the establishment and supervision of these institutions will be carried out by the Capital Markets Board, and the minimum standards required for the establishment of these institutions have been determined. With the addition of Article 35/C to the Law, the procedures for conducting these crypto asset transactions have been regulated. Furthermore, alongside other provisions, Articles 99/A and 99/B regulate the sanctions for unauthorized activities and the procedures for supervising these institutions.

The criminal law aspect of the regulation in question has been established through Article 109/A of the Capital Markets Law (SPK), which regulates the offense of “Unauthorized Provision of Crypto Asset Services”, and Article 110/A, which regulates the offense of “Embezzlement in Crypto Asset Service Providers”. Therefore, from the moment this Law came into effect, individuals engaging in these actions will be penalized under the aforementioned offenses. In this way, it is intended to put an end to doctrinal and practical debates on this matter, as well as to practices that violate the principle of legality in crime and punishment.

As can be seen, this Law does not include a specific provision regarding the use of crypto assets in the laundering of proceeds of crime, nor is there any need for such a provision. The offense of laundering, regulated under Article 282 of the Turkish Penal Code (TCK), is already sufficient in scope and is broadly formulated to encompass all forms of conduct. Furthermore, the use of crypto assets in committing this offense does not constitute a new crime but rather represents a new method of committing an existing offense. However, the regulations introduced in the Capital Markets Law (SPK) concerning the issuance and operation of crypto assets, as well as the regulation of intermediary institutions, and particularly the designation of the Capital Markets Board as the supervisory and oversight authority, are crucial for tracking potential money laundering activities. Through these regulations, the Financial Crimes Investigation Board (MASAK) can implement the KYC/AML regime both directly and via the Capital Markets Board on these intermediary institutions. Therefore, we find this regulation to be highly appropriate and beneficial, as it not only brings order to the crypto asset sector and prevents significant grievances experienced in the past but also facilitates the implementation of rules related to the prevention of money laundering and the financing of terrorism.

As we have mentioned above, the key nodes in the fight against the laundering of proceeds of crime and the financing of terrorism, as well as in the implementation of the KYC/AML regime, are the intermediary institutions that facilitate fund transfers or transactions. These are broadly defined as “obliged parties” in our legal framework. Obligated parties are specified in Article 2/1-d of Law No. 5549 on the Prevention of Laundering Proceeds of Crime and in Article 4/1 of the Regulation on Measures Regarding the Prevention of Laundering Proceeds of Crime and Financing of Terrorism (Measures Regulation). With the amendment published in the Official Gazette No. 31471, dated 01.05.2021, subparagraph (ü) was added to Article 4, paragraph 1, of the Measures Regulation, and as of this date, “crypto asset service providers” have been included among the obliged parties.

Indeed, it is explicitly stated in the May 2021 guide¹⁴⁹ titled “*Fundamental Principles Regarding Obligations on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism*”, issued by the Financial Crimes Investigation Board (MASAK) for crypto asset service providers, that obliged parties are “the most important stakeholders of MASAK in the fight against crime.”

The obligations imposed on crypto asset service providers include customer identification, reporting suspicious transactions, providing information and documents, continuous reporting, and retention and submission of records. Failure to fulfill these obligations results in various administrative fines.

As can be seen, prior to the regulation of crypto assets and intermediary institutions by law, MASAK had already included intermediary institutions within the scope of obliged parties. After the regulation of these assets and institutions by law, the obligations imposed by MASAK can be enforced more rigorously.

Conclusion

Crypto assets are digital asset units that exist solely in digital form, typically without a central issuing or regulatory authority, instead utilizing a decentralized system to record transactions. Despite the absence of trusted third-party intermediaries or oversight, these assets operate in a global, permanent, and censorship-resistant digital environment that ensures transaction integrity and speed through cryptographic principles. In fact, due to their reliance on anonymous users and decentralized management, operating on DLT without accountability or the need to obtain permission from any location, crypto assets have a higher potential for being used to launder proceeds of crime compared to traditional payment methods and are more susceptible to misuse.

As a rule, the possession and use of crypto assets do not constitute a crime; however, this does not mean that these assets cannot be used in the commission of crimes. These

¹⁴⁹ (Online) <https://masak.hmb.gov.tr/rehberler>, (accessed) 17.07.2024, p. 6.

tools can be utilized in the commission of many crimes, particularly those committed for economic gain. Indeed, the frequent association of crypto assets with various crimes in Türkiye in recent days is for this very reason.

Crypto assets are most frequently associated with the offenses of money laundering and financing of terrorism. The reason for this is that these tools possess features such as anonymity and difficulty in tracking, which are essential for laundering processes. Indeed, there are serious concerns that the anonymity provided by crypto assets and the lack of regulation facilitate money laundering, tax evasion, drug trafficking, and other criminal activities. Another significant factor is that transactions conducted with crypto assets do not fall under a single jurisdiction and lack a central intermediary. This creates a legal uncertainty that makes it challenging to properly control, record, investigate, and prosecute criminal activities arising from this technological innovation.

When criminals engage in laundering activities using crypto assets, they often employ various methods such as crypto asset tumblers, mixing services, peer-to-peer (P2P) networks, OTC brokers, and the exploitation of DeFi platforms. Although their approaches differ, all these methods serve the same purpose: concealing the original source of the proceeds of crime and making it more difficult for law enforcement to trace.

Crypto assets have significant potential for use in laundering proceeds of crime. However, this does not mean that this potential has been fully realized. Therefore, the existence and development of the technology and the crypto asset ecosystem should not be hindered or eradicated solely due to this potential. Additionally, it should not be forgotten that completely banning such technology could drive it underground.

The Financial Action Task Force (FATF) is the leading organization worldwide in combating money laundering and the financing of terrorism. For this reason, through its work and the guidelines it issues specific to this area, FATF serves as a guide for lawmakers and practitioners around the world in the fight against money laundering and the financing of terrorism. With this role and the authority, it derives from it, FATF has published various guidelines regarding the use of crypto assets in money laundering and the financing of terrorism. The conclusion drawn from these guidelines, as explicitly stated by the organization itself, is to approach crypto assets with a “risk-based” perspective.

We must express that we find FATF’s risk-based approach to be appropriate. However, this perspective does not imply a prohibition on the part of FATF, nor should it evolve into a prohibitive mindset for countries aiming to align with FATF’s approach and recommendations on this matter. The risk-based approach is correct because, at present, crypto assets are not as intensively used for money laundering as often exaggerated, but it is a fact that they carry this potential if not controlled. For this reason, FATF has developed a risk-based approach to address this potential situation.

We must express that, in the final analysis, we do not support FATF's extreme approach regarding the complete prohibition of crypto asset activities, if deemed necessary. There are two reasons for this: First, such a prohibition would hinder technological progress. This would, in turn, prevent innovation and obstruct efforts to explore ways for better and more prosperous living. Once such prohibitions begin, they tend to spread under various justifications, which ultimately impedes the progress of science, technology, and humanity. Second, such a normative prohibition would lack practical applicability in real life. In other words, such a restrictive norm is doomed to fail in terms of social effectiveness.

Individuals involved in laundering proceeds of crime are increasingly using crypto assets to launder funds obtained from various criminal activities. Tracing these illicit funds back to their source has become a challenging task for law enforcement, as they often rely on traditional investigative methods that are not suited to the characteristics of crypto assets. The use of crypto assets during the stages of placement, layering, and integration in the laundering process makes these operations even more complex and harder to track. Criminals utilize crypto asset tumblers and mixing services to obscure the origins of their illicit gains, further complicating law enforcement's efforts to trace the flow of money and identify the perpetrators of the crimes.

Law enforcement must have access to state-of-the-art tools and techniques to effectively combat laundering operations conducted through crypto assets, trace proceeds of crime, and identify perpetrators. This is especially crucial given the unique nature of crypto assets, their decentralized structures, and the anonymity they can offer to users. Traditional methods for tracing and tracking proceeds of crime are often inadequate in the face of these challenges, necessitating the development and adoption of advanced investigative techniques specifically tailored to the field of crypto assets.

In addition to these advanced tools and techniques, law enforcement must have access to comprehensive and timely information. This requires close cooperation with crypto asset intermediary institutions, financial institutions, regulatory bodies, and other relevant stakeholders. Through information sharing and joint efforts, a more transparent and secure crypto asset environment can be created, making it more difficult for criminals to exploit it for laundering proceeds of crime and engaging in other illegal activities. In Türkiye, crypto assets and crypto assets intermediary institutions were regulated through amendments to the Capital Markets Law (SPK) No. 6362, dated 06.12.2012, under Law No. 7518, dated 26.06.2024. The criminal law aspect of the regulation was established through Article 109/A of the SPK, which regulates the offense of "Unauthorized Provision of Crypto Asset Services", and Article 110/A, which regulates the offense of "Embezzlement in Crypto Asset Service Providers". Therefore, from the moment this Law came into effect, individuals engaging in these actions will be penalized under the aforementioned offenses. In this way, it is aimed to put an end to doctrinal and practical debates on this matter, as well as to practices that violate the principle of legality in crime and punishment.

As can be seen, this Law does not include a specific provision regarding the use of crypto assets in the laundering of proceeds of crime, nor is there any need for such a provision. The offense of laundering, as regulated under Article 282 of the Turkish Penal Code (TCK), is sufficiently comprehensive in scope and broadly formulated to encompass all forms of conduct.

Intermediary institutions facilitating fund transfers or transactions are key nodes in the fight against money laundering and the financing of terrorism and play a central role in implementing the KYC/AML regime. These entities are defined more broadly in our legal framework as “obliged parties”. According to the amendment made to Article 4, paragraph 1, of the Regulation on Measures Regarding the Prevention of Laundering Proceeds of Crime and Financing of Terrorism, published in the Official Gazette No. 31471 on 01.05.2021, subparagraph (ü) was added, and “crypto asset service providers” were included among the obliged parties as of this date.

The obligations imposed on crypto asset service providers include customer identification, reporting suspicious transactions, providing information and documents, continuous reporting, and record retention and submission. Failure to fulfill these obligations results in various administrative fines.

In summary, while crypto assets present both opportunities and risks, efforts should be made to prevent their use in money laundering and the financing of terrorism, while ensuring that this technological advancement and the benefits it provides are not hindered. It is gratifying to see that Türkiye’s legislation has so far been shaped in line with this perspective.

References

- Akbulut**, Berrin, “Kripto Para ve Terörizmin Finansmanı,” *Karşılaştırmalı Hukukta ve Türk Hukukunda Terörizm, Terör Suçları ve İnfaz Hukuku*, ed. İzzet Özgenç, Vol. I, Türkiye Bilimler Akademisi, Ankara, 2024.
- Aslam**, Sidra / Tošić, Aleksandar / Mrissa, Michael, “Secure and Privacy-Aware Blockchain Design: Requirements, Challenges and Solutions,” *Journal of Cybersecurity and Privacy*, Vol. 1, 2021.
- Balcı**, Murat / Çakır, Kerim, *Kripto Paraların Karapara Aklama Yöntemi Olarak Kullanılması*, CHD, Year: 16, Issue: 46, August, 2021.
- Brown**, Steven David, “Cryptocurrency and Criminality: The Bitcoin Opportunity,” *The Police Journal*, Vol. 89, Issue 4, 2016.
- Buttigieg**, Christopher P. / Efthymiopoulos, Christos / Attard, Abigail / Cuyle, Samantha, “Anti-Money Laundering Regulation of Crypto Assets in Europe’s Smallest Member State,” *Law and Financial Markets Review*, Vol. 13, No. 4, 2019.
- Çakır**, Kerim, *Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu*, 2nd Edition, Adalet Yayınevi, Ankara, 2023.
- Campbell-Verduyn**, Malcolm, “Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance,” *Crime, Law and Social Change*, Vol. 69, No. 2, March 2018.
- Durdu**, Erdal, *Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku*, Unpublished Master’s Thesis, Galatasaray University, 2018.
- Duyne**, Petrus C. van / Lampe, Klaus von / Passas, Nikos (eds.), *Upperworld and Underworld in Cross-Border Crime*, Wolf Legal Publishers, Nijmegen, 2002; FATF, 2015: 6.
- Dülger**, Murat Volkan / Özkan, Onur, “Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi,” *Prof. Dr. Mehmet Emin Artuk’a Armağan*, Ed. Mahmut Koca, Seçkin Yayıncılık, Ankara, 2020.
- Dyntu**, Valeriia / Dykyi, Oleh, “Cryptocurrency in the System of Money Laundering,” *Baltic Journal of Economic Studies*, Vol. 4, No. 5, 2018.
- Dyson**, Simon / Buchanan, William J. / Bell, Liam, “The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime,” *The Journal of British Blockchain Association*, Vol. 1, Issue 2, 2018.
- Forgang**, George, *Money Laundering Through Cryptocurrencies*, Unpublished Master of Science Thesis, La Salle University Economic Crime Forensics Capstones 40, 2019, p. 4, (Online) https://digitalcommons.lasalle.edu/ecf_capstones/40, (accessed: 15.06.2024).
- Greenberg**, Arnold, “The Dark Web’s Favorite Currency Is Less Untraceable Than It Seems,” *Wired*, April 23, 2018, (Online) <https://www.wired.com/story/monero-privacy/>, (accessed: 10.07.2024).
- Griswold**, Alison, “The First-Ever Bitcoin Purchase Was Remarkably Inglorious,” *Slate*, May 23, 2014, (Online) <https://slate.com/business/2014/05/first-bitcoin-purchase-two-pepperoni-pizzas-from-papa-john-s.html>.
- Işık**, Hüseyin, “Mali Eylem Görev Gücü’nün (FATF) Gri Listesi ve Türkiye,” *International Journal of Public Finance*, Vol. 7, No. 2, 2022.

Jacobs, Garry, "Cryptocurrencies & The Challenge of Global Governance," *Cadmus*, Vol. 3, Issue 4, May 2018, (Online) <https://cadmusjournal.org/>, (accessed: 11.07.2024).

Jia, Kai / Zihang, Falin, "Between Liberalization and Prohibition: Prudent Enthusiasm and the Governance of Bitcoin/Blockchain Technology," in: *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, Ed. Malcolm Campbell-Verduyn, Routledge, London and New York, 2018.

Kharif, Olga, "Bitcoin is being dropped by criminals in favour of privacy coins like monero," *Independent*, January 2, 2018, (Online) <https://www.independent.co.uk/news/business/analysis-and-features/bitcoin-latest-updates-price-privacy-coins-cryptocurrency-monero-digital-currency-price-a8137901.html>, (accessed: 10.07.2024).

Keech, Elliott Maurice Nathaniel, *Crime, Innovation, and The Technology of Moneys*, Unpublished PhD Thesis, University of York, York Law School, York, 2022.

Kethineni, Sesha / Cao, Ying / Dodge, Cassandra, "Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes," *American Journal of Criminal Justice*, Vol. 43, Issue 2, May 2017.

Koshy, Philip / Koshy, Diana / McDaniel, Patrick, "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic," *18th International Conference on Financial Cryptography and Data Security*, Ed. Reihaneh Safavi-Naini/Nicolas Christin, Springer Verlag, Heidelberg, 2014.

Kurzweil, Ray, *The Singularity is Near: When Humans Transcend Biology*, Penguin, London, 2005.

Malwa, Shaurya, "\$1.2 Billion in Cryptocurrency Laundered Through Bitcoin Tumblers, Privacy Coins," July 6, 2018, (Online) <https://finance.yahoo.com/news/1-2-billion-cryptocurrency-laundered-224521652.html>, (accessed: 11.07.2024).

Manna, Michele, *The Bonfire of Banknotes*, Mercati, Infrastrutture, Sistemi di Pagamento (Markets, Infrastructures, Payment Systems) Approfondimenti (Research Papers), No. 25, Banca d'Italia, Rome, 2022.

Matthewman, Steve, *Technology and Social Theory*, Palgrave Macmillan, London, 2011.

Mayer, Maximilian / Carpes, Mariana / Knoblich, Ruth (eds.), *The Global Politics of Science and Technology – Vol. 1, Concepts from International Relations and Other Disciplines*, Springer, New York, 2014.

Mayer, Maximilian / Carpes, Mariana / Knoblich, Ruth (eds.), *The Global Politics of Science and Technology – Vol. 2, Perspectives, Cases and Methods*, Springer, New York, 2014.

Meiklejohn, Sarah / Pomarole, Marjori / Jordan, Grant / Levchenko, Kirill / McCoy, Damon / Voelker, Geoffrey M. / Savage, Stefan, "A Fistful of Bitcoins: Characterizing Payments among Men with No Names," *Communications of the ACM*, Vol. 59, Issue 4, April 2016.

Möser, Malte / Böhme, Rainer, "Anonymous Alone? Measuring Bitcoin's Second-Generation Anonymization Techniques," *2017 IEEE European Symposium on Security and Privacy: Workshops (EuroS&PW)*, 2017.

Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," October 30, 2008, (Online) <https://bitcoin.org/bitcoin.pdf>, (accessed: 11.07.2024).

Nasdaq, “Know Your Coins: Public vs. Private Cryptocurrencies,” September 22, 2017, (Online) <https://www.nasdaq.com/articles/know-your-coins-public-vs-private-cryptocurrencies-2017-09-22>, (accessed: 10.07.2024).

Noether, Shen, “Ring Signature Confidential Transactions for Monero,” *IACR Cryptology ePrint Archive*, 2015, (Online) <https://eprint.iacr.org/2015/1098>, (accessed: 16.07.2024).

Prendi, Llambi / Borakaj, Daniel / Prendi, Klarida, “The New Money Laundering Machine Through Cryptocurrency: Current and Future Public Governance Challenges,” *Corporate Law & Governance Review*, Vol. 5, Issue 2, 2023.

Pielke Jr., Roger / Wigley, Tom / Green, Christopher, “Dangerous Assumptions,” *Nature*, 452, 2008.

Ramey, Corinne, “The Crypto Crime Wave is Here,” *The Wall Street Journal*, April 26, 2018, (Online) <https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366>, (accessed: 10.07.2024).

Sasson, Eli Ben / Chiesa, Alessandro / Garman, Christina / Green, Matthew / Miers, Ian / Tromer, Eran / Virza, Madars, “Zerocash: Decentralized Anonymous Payments from Bitcoin,” *IEEE Symposium on Security and Privacy*, 2014, (Online) <https://ieeexplore.ieee.org/document/6956581>, (accessed: 16.07.2024).

Sat, Diana Mergenovna / Krylov, Grigory Olegovich / Bezverbnyi, Kirill Evgenyevich / Kasatkin, Alexander Borisovich / Kornev, Ivan Aleksandrovich, “Investigation of Money Laundering Methods Through Cryptocurrency,” *Journal of Theoretical and Applied Information Technology*, Vol. 83, No. 2, January 2016.

Sharif, Romel, “Digital Bill: An Approach to Minimize Illicit Activities and Other Drawbacks of Crypto Currency,” May 2023, (Online) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4434303, (accessed: 28.07.2024).

Stokes, Robert, “Anti-Money Laundering Regulation and Emerging Payment Technologies,” *Banking and Financial Services Policy Report*, Vol. 32, Issue 5, 2013.

Tarakçıoğlu, Zeynep Esra, “Kripto Varlıkları ve Ceza Hukuku Sorumluluğu,” *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi*, Vol. 11, Issue 2, December 2021.

Verduyn, Malcolm Campbell / Goguen, Marcel, “The Mutual Constitution of Technology and Global Governance: Bitcoin, Blockchains, and the International Anti-Money Laundering Regime,” in: *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, Ed. Malcolm Campbell-Verduyn, Routledge, London and New York, 2018.

Wegberg, Rolf van / Oerlemans, Jan-Jaap / Deventer, Oskar van, “Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin,” *Journal of Financial Crime*, Vol. 25, Issue 2, 2018.

Wirdum, Aaron van, “New EU Directive May Impose Anti-Money Laundering Regulations on Bitcoin Wallet Providers,” *Bitcoin Magazine*, 2016, (Online) <https://bitcoinmagazine.com/articles/new-eu-directive-may-impose-anti-money-laundering-regulations-on-bitcoin-wallet-providers-1468424029/>, (accessed: 09.08.2024).

Yelowitz, Aaron / Wilson, Matthew, “Characteristics of Bitcoin Users: An Analysis of Google Search Data”, *Applied Economics Letters*, Vol. 22, Issue 13, 2015.

Yermack, David, "Corporate Governance and Blockchains", Review of Finance, Vol. 21, Issue 1, March 2017

Online References

Financial Crime Academy, "Understanding Crypto Money Laundering Methods: The Cryptocurrency Crime," (Online) [https://financialcrimeacademy.org/cryptocurrency-money-laundering-methods/#:~:text=What%20are%20the%20methods%20of,decentralized%20finance%20\(DeFi\)%20platforms](https://financialcrimeacademy.org/cryptocurrency-money-laundering-methods/#:~:text=What%20are%20the%20methods%20of,decentralized%20finance%20(DeFi)%20platforms), (accessed: 10.06.2024).

https://tr.wikipedia.org/wiki/Silk_Road, (accessed: 04.07.2024).

Europol, "Illegal Network Used Cryptocurrencies and Credit Cards to Launder more than EUR 8 Million from Drug Trafficking," April 9, 2018, (Online) <https://www.europol.europa.eu/media-press/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking>, (accessed: 11.07.2024).

HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing*, October 15, 2015, (Online) <https://www.gov.uk/government/publications/uk-national-risk-assessment-of-money-laundering-and-terrorist-financing>, (accessed: 05.07.2024).

Cryptocurrency Anti-Money Laundering Report, 2018, (Online) <https://info.ciphertrace.com/crypto-aml-report-q218>, (accessed: 11.07.2024).

<https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down>, (accessed: 18.07.2024).

<https://www.justice.gov/opa/pr/bitcoin-fog-operator-convicted-money-laundering-conspiracy>, March 14, 2024, (accessed: 18.07.2024).

<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html>, July 9, 2024, (accessed: 19.07.2024).

Europol Interpol Cybercrime Conference Makes the Case for Multi-Sector Cooperation, Retrieved October 2, 2015, (Online) <https://www.europol.europa.eu/media-press/newsroom/news/europol-%E2%80%93-interpol-cybercrime-conference-makes-case-for-greater-multisector-cooperation>, (accessed: 10.08.2024).

<https://masak.hmb.gov.tr/rehberler>, (accessed: 17.07.2024).