Cryptocurrency Money Laundering: A New Challenge for the European Anti-Money Laundering Framework

Petar Ristic*

Table of Contents

Abstract

Money laundering has developed at the same pace, if not quicker, as the laws that were meant to restrain it. The advent of cryptocurrency escalated the century-long arms race between money launderers and regulators as cryptocurrencies shifted the frontline from the thoroughly governed, centralized financial sector to the (semi)anonymous, decentralized and unevenly regulated cryptocurrency domain. Recent reports indicate that cryptocurrency money laundering represents a problem of considerable proportions. Owing to the fast-paced development of the crypto ecosystem and the growing interconnectedness between cryptocurrency and the traditional financial sector, forward looking and future-proof solutions are a *conditio*

* LL.M (Europa-Institut, Saarland University, Germany) and Master of Arts (Friedrich-Alexander University, Germany); Email: petar.ristic102@gmail.com. This article is based on his Master thesis "Cryptocurrency Money Laundering: A New Challenge for the European AML Framework" supervised by Prof. iur. Dr. Christos Gortsos. The author expresses gratitude to Selka for her support during the writing process.

sine qua non for safeguarding the integrity of financial markets. Moreover, as cryptocurrency holds the promise of an accessible and expeditious transaction system, it is imperative to disperse the criminal label attached to it and work towards improving credibility through calculated regulation. Although some progress has been achieved at the EU level, European cryptocurrency anti-money laundering (AML) regulation is still in its nascent stage. European legislators have touched upon the topic of cryptocurrency in AMLD V, leaving considerable space for improvement. The objective of this study is to assess the European Union's approach to regulating cryptocurrencies from an AML perspective and propose ways forward.

Keywords: Cryptocurrency, Anti-Money Laundering, European AML Framework, AMLD V, Blockchain Analytics, Bitcoin, Blockchain, FATF, Deanonymization, Financial Crime

A. Introduction

Although the term money laundering is of a relatively recent date,[1] the act of disguising the source of illicit proceeds has been a part of economic reality for a very long time. Since the beginning of its regulation, money laundering has developed at the same pace, if not quicker, as the laws that were meant to restrain it. Importantly, as commerce started to digitalize and enter the domain of cyberspace- money laundering was quick to follow.

With the introduction of cryptocurrency,[2] a decentralized and convertible subvariant of virtual currency, an alternative to the intermediated and centralized traditional financial markets came to light. However, criminals were quick to recognize the potential to use cryptocurrency for nefarious deeds, such as money laundering. Recent reports and news findings clearly indicate that cryptocurrency money laundering represents a problem of considerable proportions.[3] In fact, the advent of cryptocurrency has escalated the century-long arms race between money launderers and regulators. Cryptocurrencies have, in a certain sense, relocated the front line from the thoroughly governed and centralized financial sector to the (semi)anonymous, decentralized and unevenly regulated cryptocurrency-ecosystem.

1 *Villanyi*, Money Laundering, History, Regulations and Techniques, 26/4/2021, available at: https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-708 (22/3/2023), p. 1, indicating that the first, well-documented, usage of the phrase dates back to the 1970s Watergate scandal.

2 Throughout the thesis, the terms cryptocurrency and crypto are used interchangeably.

3 *Chainalysis team*, Crypto-crime report: Cryptocurrency money laundering, available at: https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/ (22/3/2023), indicating how cybercriminals laundered USD 8.6 billion in 2021, constituting a 30% increase from the previous year; See also: *Silva*, Criminals hide billions in crypto cash- Europol, available at: https://www.bbc.com/news/technology-43025787 (22/3/2023), stating how, in Europe, 3 to 4 billion pounds of criminal money end up laundered through cryptocurrency.

To tackle the reinvigorated financial crime, many countries began developing new and adapting existing legislation. However, as there has been very little supranational synchronicity regarding cryptocurrency regulation, a state of regulatory disparity has emerged. Although some progress has been achieved at the level of the EU, European cryptocurrency anti-money laundering (hereinafter AML) regulation is still in its nascent stage. Indeed, the European legislators have touched upon the topic of cryptocurrencies in one of the three AML directives presently in force, leaving considerable space for improvement.

The objective of this paper is to answer the following research question: How has the EU addressed money laundering risks associated with cryptocurrency and what are the possibilities of enhancing the existing European framework to facilitate a more effective regulatory response to the threat of crypto money laundering?

This study consists of four sections. The first section elaborates on the two main concepts of the study, money laundering and cryptocurrency. It sets out to contextualize money laundering by defining the offense as well as its stages of perpetration. In addition, the section examines cryptocurrency, its features and technological underpinnings. Finally, it sets out to investigate cryptocurrency money laundering, an age-old crime reinvigorated through cutting edge technology. The subsequent section evaluates the existing European AML framework, structured around AMLD V, in its response to the financial crime and aims to identify chief trends, loopholes and obstacles in regulation. Furthermore, it analyses the most recent legislative proposals that the European Commission has brough forward, i.e., the three legislative proposals constituting the EU rulebook and the MiCA Regulation. Lastly, it investigates the way in which the FATF, the principal anti-money laundering/countering the financing of terrorism standard setting body, has addressed the matter of cryptocurrency regulation. The final section summarizes the main findings and provides recommendations for improving the present European AML regime.

B. Contextualization: Money Laundering, Cryptocurrency and Crypto Money Laundering

I. Money Laundering: Definition and Stages of Perpetration

Money laundering represents a matter of international concern that threatens to compromise the integrity of national economies and financial sectors as well as the wellbeing of nations. The United Nations Office on Drugs and Crime estimates that criminals launder between two and five percent of the global Gross Domestic Product each year, an amount ranging from USD 800 billion to 2 trillion.[4]

Despite its graveness, there is no universally accepted definition of money laundering, meaning that its comprehension differs, to an extent, in each country where

4 *United Nations Office on Drugs and Crime*, "Money Laundering", available at: https://www.unodc.org/unodc/en/money-laundering/overview.html (22/3/2023).

it considered a crime.[5] Nevertheless, supranational efforts to address the offense brought forth the 1988 Vienna Convention, which provides a useful definition. It describes money laundering as the:

> Conversion or transfer of property, knowing that such property is derived from any offense(s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offense(s) to evade the legal consequences of his actions.[6]

According to this definition, money laundering consists of the physical element of: 1) converting or transferring crime-derived property, with the aim of obfuscating its source or, alternatively, 2) assisting another person to perpetuate the offense; while the mental element includes knowledge that the property originated from a prior (underlying) offense. Finally, the term "property" refers to an "asset of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets."[7]

The crime of money laundering can be dissected into three discernable stages,[8] which follow the perpetration of a predicate criminal offense.[9] Such an offense represents a component of a separate (primary) crime, and it generates illicit proceeds that are the object of money laundering.[10] After the predicate offense has been perpetrated, the insertion of crime proceeds into the legitimate financial system takes place. This is the first stage of the money laundering process, known as placement. In practice, various methods can be utilized to facilitate placement, some of which are rather straightforward, e.g., opening a bank account and depositing criminal funds through a technique known as "smurfing".[11]

Once criminal funds enter the financial system, the stage is set for the layering phase. The objective of layering is to divorce the funds from their criminal roots by, e.g., facilitating multiple cross-border wire transfers of funds to accounts opened with banks located in offshore jurisdictions to thwart law enforcement efforts to trace the proceeds back to the original perpetrator(s).[12] Importantly, after the pro-

5 *Hetzel*, in: Reichel and Randa (eds.), pp. 119–120.
6 *UN Economic and Social Council (ECOSOC)*, United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 19 December 1988, Art. 3.1. b) i).
7 Ibid., Art. 1-q.
8 *Schott*, p. 17.
9 For a substantial period of time, drug-related crimes represented the sole predicate offense to money laundering; however, there are now more than twenty different offenses ranging from theft and robbery to cyber and environmental crimes that have been classified as predicate offenses to money laundering, see: Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ L 284 of 12/11/2018, Art. 2.
10 *Rossel* et al., in: Unger et al. (eds.), p. 240.
11 Smurfing involves cash couriers, so-called *smurfs*, who are instructed to break down large sums of dirty money through small-scale bank deposits that are inconspicuous and avoid triggering the filing of cash transaction reports, see: *Madinger*, p. 332.
12 *Madsen*, p. 106.

cess of layering comes to an end, a semblance of legality of earnings arises, i.e., the dirty funds appear to have been cleaned.

Integration, the final stage of money laundering, signals the re-entering of layered, ostensibly clean funds into mainstream commerce, where they become intertwined with lawful earnings.[13] Similarly to layering, integration is facilitated through a variety of methods, all of which aim to enable criminals to dispose of their funds in the least conspicuous way.[14] By this stage the offender is able to use the laundered funds to purchase luxury items, real estate and other goods or services.

II. Cryptocurrency

Due to its ever-evolving nature, it is difficult to propose a stable definition of virtual currency.[15] In one of its reports, the FATF defined virtual currency as a:

> Digital representation of value that can be digitally traded and functions as 1) a medium of exchange; and/or 2) a unit of account; and/or 3) a store of value, but does not have legal tender status in any jurisdiction.[16]

Since El Salvador and the Central African Republic classified bitcoin as legal tender,[17] the FATF definition is partly outdated regarding point three; nevertheless, it remains highly instructive. In essence, virtual currency constitutes a computerized (non-tangible) form of value that exists within a virtual system. This value can be digitally traded and depending on whether it is tradable for fiat or other virtual currencies (or some other asset), it can be classified as non-convertible,[18] or convertible. According to the FATF, convertible virtual currency can be further split into centralized and decentralized, depending on whether there exists a central administrator, empowered to issue the virtual currency, withdraw it, and oversee the digital system as a whole.[19]

13 *Richards*, pp. 49 ff.
14 *Smyczek*, in: Chadraba and Springer (eds.), pp. 497–498.
15 For example, in 2012 the European Central Bank proposed a definition that was revised only three years later. In fact, owing to increased regulation of virtual currencies in a number of jurisdictions, it was no longer meaningful to define virtual currencies as "unregulated" as the ECB did in 2012. See: *European Central Bank*, Virtual Currency Schemes – a further analysis, ECB 2015, p. 25.
16 *FATF*, Virtual Currencies: Key Definitions and potential AML/CFT Risks, 2014, p. 4.
17 *The Economist*, Using bitcoin as legal tender. available at: https://www.economist.com/finance-and-economics/2021/09/04/using-bitcoin-as-legal-tender (22/3/2023), and *CNBC*, Central African Republic becomes second country to adopt bitcoin as legal tender, available at: https://www.cnbc.com/2022/04/28/central-african-republic-adopts-bitcoin-as-legal-tender.html (22/3/2023).
18 Coins used in massive multiplayer online role-playing games (e.g., Silkroad Online, Guild Wars) are non-convertible virtual currencies. These coins are used by players to purchase in-game items that help them advance through the game. However, trading these coins is strictly prohibited outside the virtual game setting and may lead to account termination.
19 *FATF*, *FATF*, Virtual Currencies: Key Definitions and potential AML/CFT Risks, 2014, p. 5.

Cryptocurrency can be defined as convertible decentralized virtual currency; accordingly, it represents a sub-variant of the broader concept of virtual currency. Cryptocurrency can be traded for fiat and other (convertible) virtual currency. There is no underlying central authority to administrate the system and supervise its workings. However, as is the case with money laundering, there is no single universally accepted definition of what constitutes cryptocurrency; in fact, most policy makers have not bothered with defining the concept.[20]

The following sub-chapter will primarily focus on Bitcoin,[21] the first and most-successful cryptocurrency to date. What is more, the decision to focus on Bitcoin is driven by the finding that it represents the most frequently used cryptocurrency for money laundering/terrorist financing purposes.[22]

1. Bitcoin and Blockchain Technology

In 2008, against the background of global financial distress and mounting distrust towards financial institutions, a person under the pseudonym of Satoshi Nakamoto published a document proposing an alternative to the mainstream financial system. Nakamoto's radical proposal was Bitcoin, a "peer-to-peer version of electronic cash" that would operate as a decentralized system completely ridden of any intermediation from financial institutions.[23]

In essence, a non-centralized network of peers would generate the virtual currency,[24] process and verify irreversible transactions and maintain a public record/ledger of all past and ongoing transaction activity. Admittedly, it was not the first undertaking of its kind;[25] however, what made Bitcoin stand out was the intricate distributed ledger technology laying at its core, known as blockchain. In simple terms, blockchain represents a database of transactions that is shared between system participants, referred to as nodes, which form a global network that is engaged in the verification of transactions.[26] There are two key components of blockchain technology: asymmetric cryptography and a mechanism known as Proof-of-Work.

20 *Houben/Snyers*, Cryptocurrencies and Blockchain: Legal context and implications for financial crime, money laundering and tax evasion, available at: https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1/language-en (22/3/2023), p. 23.

21 As is the practice in academic circles, the word "Bitcoin" shall be used to refer to the protocol/ecosystem as a whole, while "bitcoin" will be used to refer to the currency, i.e., bitcoin as a means of exchange.

22 *FATF*, Second 12-Month review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html, (22/3/2023), para. 98.

23 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, available at: available at: https://bitcoin.org/bitcoin.pdf (23/3/2023), p. 1.

24 The first fifty bitcoins were created by Nakamoto himself, see: *Simser*, JFC 2015/2, p. 161.

25 For a concise overview, see: *Sathya/Elngar*, in Panda et al. (eds.), pp. 3–4.

26 *Judmayer et al.*, p. 30.

Asymmetric cryptography secures the anonymity of the Bitcoin payer (i.e., sender) and payee (i.e., receiver). It represents a system based on the idea that each network user holds a unique keyset, containing a public and private cryptographic key.[27] A public key can be compared to a bank account and it represents the address of a user's wallet, where cryptocurrency can be stored. It is visible to all network participants and enables data encryption as well as signature verification. It does not, however, disclose any personal information of the address owner.[28] The private key is secret, known exclusively by the owner, and its purpose is to decrypt information and digitally sign transactions.

Following their creation, bitcoin transactions are released into the open network where they are verified. Transaction verification takes place thanks to a process known as 'mining'. Network nodes, known as miners, attempt to generate hashes,[29] with a numerical value lower than or equal to a specified target. As soon as a valid hash is mined, the transaction becomes verified and ends up stored in a one-megabyte block of data. In addition, the fastest miner to generate the valid hash is given a reward in the form of new bitcoins, which serve as an incentive to engage in the mining process.[30] Importantly, the extensive computational effort that goes into the mining activity constitutes Proof-of-Work, the second component of blockchain.

Over time Bitcoin has developed a *sui generis* commercial ecosystem that encompasses numerous entities, e.g., users, miners and service providers such as tumblers, virtual currency exchanges, trading platforms and wallet providers. In addition, it is worth mentioning that bitcoin has no intrinsic value and is quantitatively finite.[31] Accordingly, the price of bitcoin predominantly depends on what users are willing to pay for it.[32] This has caused considerable price volatility and has led some commentators to draw similarities between bitcoin and the dot com stocks of the nineties.[33] However, unlike most of the aforementioned stocks, Bitcoin continues to exists and has accumulated a considerable pool of users.[34] Importantly, Bitcoin has become more accepted and is now recognized as a form of payment by a number of

27 A cryptographic key is a large string of random characters that is fed through an algorithm to scramble or (in case of a private key) unscramble data, See: *Vacca*, p. 120.

28 *Hencic and Gourieroux*, in: Huynh et al. (eds.), p. 19.

29 A hash represents algorithmic output in the form of a unique string of characters that is produced when data is fed into the algorithm, see: *Bazan-Palomino*, in: Pichl et al. (eds.), pp. 238–239.

30 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, available at: available at: https://bitcoin.org/bitcoin.pdf (23/3/2023), p. 4.

31 *Bitcoin Project* (2009-2022), What is Bitcoin?, available at: https://bitcoin.org/en/faq#doesnt-bitcoin-unfairly-benefit-early-adopters (19/1/2023), the limit is set at 21 million bitcoins.

32 Ibid., indicating how the law of supply and demand drives the value of bitcoin.

33 *Simser*, JFC 2015/2.

34 See: *De Best*, Estimate of the number of identity-verified cryptoasset users from 2016 to November 2022, available at: https://www.statista.com/statistics/1202503/global-cryptocurrency-user-base/ (22/3/2023), indicating that there are more than 400 million users worldwide.

notable companies such as PayPal and Microsoft, which has undoubtably exerted a positive effect on its credibility.[35]

2. Bitcoin's Pseudo-anonymous Nature

Anonymity refers to the characteristic of being unidentifiable or untraceable. Owing to the anatomy of Bitcoin's underlying blockchain technology, users are provided with a certain degree of anonymity. Firstly, since transactions take place on a decentralized peer-to-peer basis, financial intermediaries, such as banks, are barred from any processing activity and the payer/payee do not have to disclose any private information before, during or after the transaction. Secondly, addresses assigned to Bitcoin users are anonymous, meaning there is nothing that can directly link an address to a real-world identity.[36] What is more, Bitcoin users can hold more than a single address and are even encouraged to, as a matter of good practice, create a new address each time they engage in a new transaction.

However, Bitcoin does not secure absolute anonymity; in fact, anonymity is eroded to a considerable extent because every single verified transaction becomes integrated into the public blockchain. Therefore, the entire transaction history becomes openly visible and traceable.[37] Such a degree of transparency is suitable for the application of blockchain analytic tools, incorporating behavior and transaction-based clustering techniques, that have proven effective in identifying users behind crypto addresses.[38] In fact, deanonymization can be executed by linking *prima facie* anonymous users to external, off-grid data sources that can disclose personal details, such as email and shipping addresses.[39] Moreover, a study by *Juhasz et al.* has indicated the possibility of connecting a user's Bitcoin address to their IP address, which would then enable determining an individual's geographic location.[40] Therefore, contrary to popular belief, Bitcoin and the majority of other cryptocurrencies relying on analogous (public) blockchain technology provide their users with limited anonymity.

The limited anonymity of cryptocurrencies relying on transparent blockchain technology has triggered the emergence of privacy coins. Privacy coins represent a type of cryptocurrency that incorporates technological solutions that obfuscate their ledger. Consequently, the sender/receiver and transacted amount become hid-

35 *Walsh*, Paying with Bitcoin: These are the major companies that accept cryptos as payment, available at: https://www.euronews.com/next/2021/12/04/paying-with-cryptocurrencies-these-are-the-major-companies-that-accept-cryptos-as-payment (22/3/2023).

36 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, available at: https://bitcoin.org/bitcoin.pdf (23/3/2023), p. 6.

37 *Zhang*, in: Pompella and Matousek (eds.), p. 252.

38 *Androulaki et al.*, FCDS 2013/7859, p. 51.

39 *Reid and Harrigan*, in: Altshuler et al. (eds.), p. 212 ff., the authors point to information stored by virtual currency exchanges, businesses excepting bitcoin as payment, online forums etc.; a similar conclusion is reached in: *Reynolds/Irwin,* JMLC 2017/2, pp. 181–184.

40 *Juhasz et al*, PLoS ONE 2018/12, p. 18.

den.[41] Owing to the anonymity-enhancing features of privacy coins it is difficult to estimate the exact scale of their usage.[42] Nevertheless, privacy coins, such as Monero and Zcash, have emerged as the "cryptocurrency of choice" for criminal actors[43] and have aggravated the threat of money laundering.[44]

III. Crypto Money Laundering

Cryptocurrency money laundering represents the use of cryptocurrency to launder proceeds obtained through the commission of an underlying criminal offense. A 2022 report states that up to USD 33 billion in crypto was laundered in the period from 2017 to 2021.[45] Accordingly, it can be argued that cryptocurrency represents a valuable *modus operandi* for money laundering purposes.

Cryptocurrencies possess three key traits that make them attractive to money launderers, first of which is their decentralized nature. As cryptocurrency transactions take place outside the domain of conventional finance, within a decentralized network, AML measures cannot be applied in the same fashion as there are no (traditional) financial entities to apply them in the first place. The second characteristic pertains to user anonymity. The extent of anonymity that is given to cryptocurrency users, ranging from partial to absolute, makes it difficult to conduct AML measures.[46] This is particularly the case with privacy coins. Finally, due to the over-regulated nature of the conventional financial sector, money launderers have a strong incentive to relocate to the less regulated domain of cryptocurrency.[47] So far, regulatory responses to cryptocurrency have been diversified, ranging from outright bans (e.g., Bangladesh and China), to discouraging the use of crypto (e.g., Saudi Arabia and Jordan) to more nuanced approaches observable in the EU.[48] Importantly, the concern is that criminals could take advantage of said regulatory heterogeneity by engaging in regulatory arbitrage.

Crypto money laundering does not necessitate any radical rethinking of the money laundering concept. As with conventional money laundering, the process begins

41 *Europol*, Cryptocurrencies: Tracing the Evolution of Criminal Finances, available at: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances (22/3/2023), p. 9.
42 Ibid., p. 7.
43 *Arslanian*, p. 147, indicating that 45% of all dark net markets now support Monero, according to available reports.
44 *Kizza*, p. 551.
45 *Chainalysis Team*, The 2022 Crypto Crime Report, available at: https://go.chainalysis.com/2022-Crypto-Crime-Report.html (22/3/2023), p. 11.
46 *Campbell-Verduyn*, CLSC 2018/2, p. 287, the author points out that cryptocurrencies invert the traditional problem of parties known-transactions unknown to transactions known-parties unknown.
47 *Teichmann and Falker*, JMLC 2021/24, pp. 91, 95–96.
48 *Kepli and Zulhuda*, in: Oseni et al. (eds.), p. 255, See also: *Chohan*, Accessing the Differences in Bitcoin and other Cryptocurrency Legality Across National Jurisdictions, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3042248 (22/3/2023), pp. 4–8.

with the execution of a predicate crime, which can be classified as off-chain or on-chain. Off-chain predicate crimes take place off-line, in the real world, and primarily generate cash, while on-chain predicate offenses refer to cybercrimes that generate fiat and/or cryptocurrency.[49] In the subsequent placement phase, illicit funds are used to purchase cryptocurrency. Importantly, the entire placement step is bypassed in cases involving on-chain predicate crimes that result in the acquisition of cryptocurrency, as there is no need to make the initial crypto purchase. Following successful placement, criminals engage in intricate transactions devised to misdirect law enforcement authorities and create a facade of legality.

To better understand how layering and integration work when crypto is implicated, a recent case involving a married couple accused of laundering USD 4.5 billion in bitcoin shall be examined. Ilya Lichtenstein and his wife Heather Morgan allegedly took part in the 2016 cyberattack on the cryptocurrency exchange Bitfinex, which resulted in the theft of 119,754 bitcoins, which were then transferred to a virtual wallet held by them. Subsequently, the couple engaged in diverse layering strategies that aimed to clean the stolen bitcoins.

One of the methods used, known as the "peel-chain technique", involved moving the stolen bitcoins through a long chain of transactions, so that after each subsequent transaction a small and inconspicuous slice of bitcoin "peeled" off the chain straight into a separate account.[50] The accused pair opened multiple such accounts on a dark-web platform called Alphabay, which is well-known as a large market for illegal goods and services.[51] Importantly, the platform provided its users with its own anonymity-enhancing tumbling service. A tumbler takes multiple simultaneous transactions and mixes their streams so that it becomes difficult to link the tainted crypto with the sending address.[52] Lichtenstein and his wife availed themselves of Alphabay's tumbling software, thereby adding another level of layering to their operations, and proceeded to move their scrambled bitcoins into accounts opened on virtual currency exchanges (hereinafter VCEs) scattered across multiple jurisdictions.[53] Moreover, the aforementioned VCE accounts were created using false personal data, in an attempt to frustrate AML measures applied by the exchanges.[54] Furthermore, the VCEs where Lichtenstein and Morgan opened their accounts were used to exchange some of the stolen bitcoins for monero, a well-known

49 For example: cybertheft that targets a virtual crypto wallet or exchange. In addition, many crimes, such as the sale of drugs and illegal substances, have found their way into the virtual environment, see: *Khatri*, New York State Sees First Conviction for Crypto Money Laundering, available at: https://www.coindesk.com/markets/2019/04/24/new-york-state-sees-first-conviction-for-crypto-money-laundering/ (22/3/2023), reporting how two men were convicted for selling drugs and other illegal substances in exchange for cryptocurrency on the dark web.

50 *USAO District of Columbia*, Statement of facts in case 1:22-mj-00022, available at: https://www.justice.gov/usao-dc/press-release/file/1470221 (22/3/2023), p. 5.

51 *Kethineni*, in: Reichel (ed.), p. 161.

52 *Karame/Androulaki*, p. 98.

53 *USAO District of Columbia*, Statement of facts in case 1:22-mj-00022, available at: https://www.justice.gov/usao-dc/press-release/file/1470221 (22/3/2023), paras. 11 and 12.

54 Ibid., paras. 22, 34 and 37.

privacy coin that relies on a type of cryptography technology that completely shields transaction parties. In other words, the sender, receiver and transaction amount remain fully anonymous.[55] The aforementioned tactic of converting one cryptocurrency to another, more anonymous, is defined as "chain-hopping".

Once the couple finalized the layering strategies, they began to liquidate a considerable amount of their clean bitcoins through VCEs and Bitcoin ATMs, electronic terminals that allow users to convert bitcoin to cash and vice versa.[56] In addition, Lichtenstein bought gold and purchased Walmart, Uber and PlayStation gift cards through a VCE. Ultimately, law enforcement was able to find and arrest the couple. Authorities were able to obtain a file in Lichtenstein's cloud storage containing the private keys for the accounts opened on various VCEs.[57] These confiscated private keys enabled investigators to access the wallets and trace the stolen cryptocurrency back to the accused pair.

The case of Lichtenstein and Morgan raises some concern. It shows how a tech-savvy couple without any apparent institutional backing, or ample financial resources, was able to make use of various tools within the crypto ecosystem to (allegedly) execute a crime which, once unraveled, resulted in the largest financial seizure in US history.[58] It is hard to predict whether their endeavor will serve as an inspiration for prospective criminals to engage in similar activities from the confines of their home; nevertheless, it seems certain that money launderers are beginning to capitalize on cryptocurrencies.

C. Cryptocurrency Regulation in the European AML Framework

I. Tackling Money Laundering in the EU

The European AML regime has been developed over a period of three decades. *In toto*, it encompasses six directives, three of which are presently in force. The directives aim to: 1) preserve the soundness and stability of credit and financial institutions as well as the integrity and stability of the financial sector as a whole, 2) prevent the erosion of public trust in the financial system, and 3) decrease the levels of organized crime elevated through unfettered money laundering.[59] The directives envisage a harmonized, union-wide approach to money laundering regulation while ac-

55 Ibid., paras. 18 and 21, see also: *Kermitsis et al*., in: Akhgar et al. (eds), p. 96.
56 Ibid., paras. 24 and 31.
57 Ibid., paras. 51–55.
58 *Tucker et al*., US says $5b seizure of stolen bitcoin is largest in history, available at: https://www.pbs.org/newshour/economy/justice-department-announces-seizure-of-3-6-billion-in-laundered-cryptocurrency-2-arrests (22/3/2023).
59 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (hereinafter AMLD IV), OJ L 141 of 05/07/2015, Preamble.

cepting the indispensability of international cooperation and coordination.[60] In addition, the EU AML framework has been designed in a manner that is heavily compliant with FATF recommendations; in fact, it represents a prime example of how international soft-law becomes integrated into regional hard law.[61] Importantly, the crux of the directives lies in the imposition of AML requirements upon so-called obliged entities.

The first directive adopted a narrow approach that solely obliges banks and credit institutions, the gatekeepers of the financial sector, to apply AML measures, i.e., apply customer due diligence (hereinafter CDD) to identify the client and beneficial owner(s) and verify their identity, establish the purpose and intended nature of the business relationship, cooperate with responsible national authorities, particularly financial intelligence units (hereinafter FIUs) and devise internal AML policies and procedures.[62] Each subsequent directive has broadened the scope of obliged entities,[63] as well as the range of crimes that are considered predicate to money laundering.[64] This progressive development can be attributed to the multifaceted and developing nature of the crime. Understandably, it is crucial for regulators to keep track of technological and financial developments that could have an impact on the anatomy of money laundering.

For the purpose of fulfilling this aspiration, the EBA was given the competence to "monitor new and existing financial activities" in order to a establish a coordinated approach to regulation.[65] As the number of European cryptocurrency users and transactions began to grow, the EBA took steps to study the phenomenon in late 2013. This effort resulted in an Opinion in which the EBA proposed the imposition of AML/CDD duties upon VCEs, while leaving the door open for the potential inclusion of other market participants.[66] Essentially, the suggestion was to: 1) expand the list of obliged entities that are required to comply with AML requirements to include VCEs and possibly other connected entities, 2) subject VCEs to registration

60 Ibid., para. 4 of the Preamble.

61 *Tsingou,* in: Mügge (ed.), p. 151, this is in accordance with the proclamation contained in the EU Directives that "Union action should continue to take particular account of the FATF Recommendations and instruments of other international bodies active in the fight against money laundering and terrorist financing", see: AMLD IV, Preamble.

62 AMLD IV, Art. 10, 13, 33, 45 and 46.

63 For example, the Second Directive has integrated insurance companies and investment firms as well as a number of other professions (e.g., real estate agents, tax advisors), See: Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, OJ L 344 of 28/12/2001, Art. 1 and 2a.

64 There are over 20 predicate offenses in the latest EU AML directive, See: Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ L 284 of 12/11/2018, Art. 2.

65 Regulation No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, OJ L 331 of 15/12/2010, Art. 9-2.

66 *European Banking Authority*, EBA Opinion on 'virtual currencies', EBA/Op/2014/08, paras. 156–157.

requirements before allowing them to provide exchange services, and 3) oblige VCEs to provide the authorities with information on beneficial owners/controllers in order to enable officials to determine whether they are "fit and proper persons".[67] However, none of these suggestions found their way into the legislation of the time and it is only with the introduction of AMLD V that the topic of cryptocurrency came into consideration.

II. Change in the Regulatory Landscape: AMLD V

In 2015 a series of terrorist attacks took place across several European states. Following these disastrous events, speculations arose that the perpetrators behind one of the Paris bombings were funding their operations through the use of bitcoin.[68] Moreover, the EU Institute for Securities Studies found that the Islamic State of Iraq and the Levant had been relying on cryptocurrencies to sustain itself financially and operate on the dark web markets.[69] In light of these events and the need to improve financial oversight, the European legislators decided to incorporate the concept of virtual currency (hereinafter VC) into AMLD V.[70]

Recital 8 of the Preamble of AMLD V is highly revealing. It indicates how the gatekeepers in control of the VC sector have not been required to identify suspicious activity and that competent national authorities have no means of monitoring VCs.[71] Accordingly, this gray area has left the door open for terrorist groups, benefiting from the lack of oversight, to easily inject their funds into European financial channels. Therefore, the legislators found it essential to begin the process of VC AML/CFT regulation by expanding the scope of obliged entities through the inclusion of: 1) providers engaged in exchange services between virtual currencies and fiat currencies (VCEs), and 2) custodian wallet providers.[72]

According to AMLD V, VCEs represent natural or legal persons that exchange virtual for fiat currency and vice versa. Coming back to the case of Lichtenstein and Morgan, it has been examined how the couple extensively relied on VCE services, e.g., to exchange stolen bitcoins for other cryptocurrency and, subsequently, liquidate their assets. What is more, in a conventional crypto money laundering scheme,

67 Ibid., paras. 162 and 163.
68 *Azain/Liv*, ICT 2018, p. 3.
69 *Berton*, The dark side of the web: ISIL's One-stop shop?, available at: https://www.iss.europa.eu/content/dark-side-web-isil%E2%80%99s-one-stop-shop (22/3/2023).
70 Proposal for a Directive of the European parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC (hereinafter AMLD V Proposal), SWD (2016) 223, p. 1.
71 Directive (EU) 2018/849 of the European parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (hereinafter AMLD V), OJ L 156 of 19/06/2018, recital 8 of the Preamble.
72 Ibid., Art. 1-1-c.

criminals utilize fiat to crypto VCEs as entry points to the crypto domain, as they enable the exchange of crime funds for crypto. Accordingly, VCEs play an important role in the placement, layering and integration stages of crypto money laundering; therefore, their inclusion into the list of obliged entities constitutes a logical first step in crypto AML regulation.

A custodian wallet provider represents "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies".[73] Cryptocurrency users are given a set of cryptographic keys that enable taking part in transactions. This keyset includes a public and a private key; the former of which is openly visible and resembles a user's bank account, while the latter is secret and is akin to a password for a bank account. There are different methods of storing the private key,[74] and one of them includes placing it in the (virtual) custody of a third party, e.g., a company operating a platform that allows users to create accounts used to deposit and administrate crypto.[75] Accordingly, as custodian wallet providers enable users to store and manage their cryptocurrency as well as engage in transfers (much like a bank does with fiat), it is meaningful to compel these entities to apply AML measures.

AMLD V instructs the two mentioned crypto-market gatekeepers to adhere to all AML/CDD requirements that have been imposed on conventional obliged entities In other words, fiat to crypto VCEs and custodian wallet providers have the duty to identify and verify the identity of the client and beneficial owner(s), determine the intended nature and purpose of the business relationship, cooperate with the authorities and so on. In this manner, national authorities and FIUs are able to monitor the usage of VCs and identify crypto wallet holders.[76]

Additionally, article 47 of AMLD V requires member states to ensure the registration of fiat to crypto VCEs and custodian wallet providers.[77] This requirement enables the authorities to examine the activities in which the obliged entities are engaged in, the money laundering/terrorist financing risks to which they are exposed and the internal mechanisms enacted to mitigate said risks.[78] Furthermore, the infor-

73 Ibid., Art. 1-2-d.

74 *Kyles*, in: Goldbarsht/de Koker (eds.), pp. 139–140, cryptocurrency can be held in hot (online) or cold (off-line) wallets; the former can be divided into custodial and non-custodial.

75 *Houben/Snyers*, in: Liaw (ed.), p. 168, custodian wallet providers enable the simplification of transactions, as users do not need to memorize their private key and only have to remember the username and password of the account they created with the wallet provider, see: *Haffke et al.*, JBR 2020/2, p. 130.

76 Basically, because of the measures, users who hold their private keys with custodian wallet providers or have accounts with VCEs cease to be anonymous.

77 AMLD V, Art. 1, para. 29.

78 Such is the case with the registration requirements in the AML framework of Luxembourg, see: *The Parliament of the Grand Duchy of Luxembourg*, Law of 12 November 2004 on the fight against money laundering and terrorist financing transposing Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering (hereinafter AML Law of 2004), Art. 7-1.

mation provided during registration enables the competent authorities to evaluate whether individuals holding managerial functions or acting as beneficial owners of obliged entities can be classified as "fit and proper persons".[79] The directive does not provide concrete guidance concerning the precise way in which this standard should be applied; nevertheless, the purpose of the evaluation appears to be the prevention of individuals associated with financial crime from taking up controlling functions, as well as ensuring that persons with said functions are of good repute and sufficient professional experience.[80]

Importantly, AMLD V sets out to define the illusive concept of virtual currency.[81] First, in recitals 10 and 11, AMLD V indicates that VCs should not be mistaken for electronic money (digitalized version of fiat), funds, monetary value stored on certain instruments defined by the Payment Services Directive, in-game currencies intrinsic to a unique game environment and local/complementary currencies, used by a limited pool of users within a small network.[82] What is more, the recital indicates how AMLD V aims to cover "all potential uses of virtual currencies" and provides a non-exhaustive list of applications.[83] Subsequently, the directive provides the following definition of virtual currency:

> a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.[84]

AMLD V defines VCs in a "technologically neutral" manner, meaning there is no requirement that VCs have to be based on a specific type of underlying technology.[85] Importantly, the definition provides several cumulative conditions, which have to be fulfilled to attain the status of VC.

From the beginning, VCs are described as fully detached from central banks or any other state-owned entity; therefore, state-backed cryptocurrency systems cannot qualify as VC.[86] The next passage indicates that VCs may or may not be connected to legally established currency; in any case, irrespective of this connection, both types fall under the umbrella of VC. Furthermore, VCs do not have legal tender status, meaning they are not used in the same fashion as legal currency, e.g., to pay tax contributions, and economic agents do not have the obligation to accept VC

79 AMLD IV, Art 47-2.
80 AML Law of 2004, Art. 7-1.
81 It should be remembered that the Directive defines the broader concept of virtual currency, which encompasses decentralized convertible virtual currencies, i.e., crypto.
82 AMLD V, recitals 10 and 11 of the Preamble, by excluding in-game currencies from the realm of virtual currency, the legislators seem to have gone against the grain of the FATF definition, which considers in-game currencies as a sub-variety of virtual currency.
83 Ibid.
84 Ibid., Art. 1-d-18.
85 *Haffke et al.*, JBR 2020/2, p. 133.
86 These are cryptocurrencies that represent state-controlled implementations of distributed ledger technology, see: *Bhatti et al.*, p. 137.

as payment for their goods/services. Moving forward, AMLD V sets out the requirement that VCs must be accepted by natural or legal persons as a means of exchange. According to *Haffke et al*., the term "means of exchange" refers to the economic function of money as an intermediary object used in trade.[87] Understandably, only those digital assets that have the capacity to facilitate the exchange of goods and services qualify as VCs.[88] Accordingly, under AMLD V, only cryptocurrencies qualify as VC and other digital assets, such as utility and investment tokens, are not to be taken into consideration.[89] Finally, the last requirements indicates that VCs must possess the capacity to be transferred, stored and traded electronically.

The inclusion of VCs into AMLD V represents an important milestone. In fact, the incorporation of VC gatekeepers into the list of obliged entities and the VC definition AMLD V put forth constitute sensible first steps towards an effective regulatory regime. The subsequent Directive 2018/1673 did not continue the work of AMLD V, and its contributions can be primarily viewed through the lens of criminal law and money laundering deterrence.[90] Possibly, the reason for the omission lies in the fact that the temporal frame between the two directives is short and the legislators did not have enough time to deliberate over the ways in which AMLD V could be improved with regard to VC regulation. In fact, Directive 2018/1673 makes a single reference to VC, found in Recital 6:

> The use of virtual currencies presents new risks and challenges from the perspective of combating money laundering. Member States should ensure that those risks are addressed appropriately.[91]

It could be argued that this passage shifts the focus from the EU to the member states, which are, rather broadly, instructed to take appropriate action to address VC risks. Ultimately, the failure to make amendments through Directive 2018/1673 has resulted in a somewhat outdated regime with several deficiencies and ambiguities that warrant reassessment.

III. Shortcomings of AMLD V

AMLD V can be criticized for not casting the net far enough to capture a number of important actors operating in the crypto ecosystem. Recital 9 of AMLD V indicates that the legislators were cognizant of this limitation by stating:

87 *Haffke et al*., JBR 2020/2, pp. 136–137.
88 Ibid.
89 Simply put, utility and investment tokens do not function as a "means of exchange". The former grant the holder access to certain applications, products or services provided within a particular crypto-ecosystem, while the latter fulfil capital raising purposes, i.e., the facilitation of an initial coin offering or "ICO", comparable to a traditional IPO, and provide holders with rights similar to dividends, see: *Houben/Snyers*, in: Liaw (ed.), p. 165.
90 Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law (hereinafter Directive 2018/1673), OJ L 284 of 12/11/2018, Art. 4, Art. 5-2, Art. 7-1 and Art. 8.
91 Ibid., Recital 6 of the Preamble.

> The inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without such providers.[92]

Firstly, AMLD V exclusively focuses on VCEs that exchange VC for fiat currency (and vice versa), while neglecting to address VCEs that facilitate the exchange of one type of VC for another. Because the legislators expected crypto money launderers to convert their crypto into cash at some point in time, natural and legal persons providing such exchange services became obvious candidates for AML regulation.[93] However, this assumption is based on the understanding that the cryptocurrency market is not able to function independently and sustain itself without fiat currency.[94] As cryptocurrency markets become more autonomous, it is no longer justifiable to solely regulate crypto to fiat exchanges. Moreover, in the previously examined case-study, it has been observed how crypto to crypto VCEs become instrumentalized in the layering stage of crypto money laundering to facilitate chain-hopping, i.e., the exchange of crime-derived crypto for clean coins. Indeed, since crypto to crypto VCEs are not qualified as obliged entities under AMLD V, they are not formally required to apply AML/CDD measures; therefore, they form a blind spot in crypto regulation that criminals are able to exploit.

Secondly, tumblers (or mixers) represent cryptocurrency service providers that also fall outside the scope of European AML legislation. To reiterate, blockchain-based transactions are publicly visible and traceable; therefore, tumblers provide a sought-after anonymity-enhancement service by obscuring the link between the crypto sender and receiver. Past studies have reported that a majority of mixer clients use such services for innocuous purposes (e.g., enhancement of financial privacy).[95] However, more recent findings have indicated an increase in the amount of

92 AMLD V, Recital 9 of the Preamble.

93 *Soana*, Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry?, 9/11/2021, Economic Notes Vol. 2022/51, available at: https://onlinelibrary.wiley.com/doi/full/10.1111/ecno.12195 (22/3/2023), pp. 3 and 8.

94 With time, major companies and other economic agents have started to accept cryptocurrency as a means of payment and users now have the possibility to use their crypto without having to exchange it for fiat currency, see *Walsh*, Paying with Bitcoin: These are the major companies that accept cryptos as payment, available at: https://www.euronews.com/next/2021/12/04/paying-with-cryptocurrencies-these-are-the-major-companies-that-accept-cryptos-as-payment (22/3/2023); See also: *Houben and Snyers*, Cryptocurrencies and Blockchain: Legal context and implications for financial crime, money laundering and tax evasion, available at: https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1/language-en (22/3/2023), pp. 33–34 and 36–37, listing a number of well-known corporates that accept cryptocurrency as a medium of exchange.

95 *Elliptic Team*, What are Bitcoin Mixers & Are They Compliant with AML Standards?, available at: https://www.elliptic.co/blog/bitcoin-mixers-assessing-risk-bitcoin-transactions (22/3/2023), a 2018 study on mixers found that only 16% of the (mixed) funds came from unlawful sources.

cryptocurrencies tumblers receive from illicit addresses.[96] Indeed, due to their potential to completely sever the link between cryptocurrency and its genuine source, tumblers have turned into a powerful *modus operandi* for crime syndicates to launder tainted cryptocurrency.[97] Accordingly, their inclusion into AMLD V would have been a welcomed development.

Thirdly, P2P trading platforms, where cryptocurrency users directly trade with one another, constitute important players in crypto markets that remain outside the scope of AMLD V. Depending on whether they are operated by a central entity or not, these platforms can be classified as centralized or decentralized. Centralized P2P platforms have an administrator that runs the platform, monitors ongoing processes, provides escrow services and functions as a central point of contact/liability for the platform. Decentralized platforms, on the other hand, operate on the basis of smart contracts, i.e., they are software-based, and as such they represent an obstacle for regulators because it is not possible to single out a concrete managerial entity to subject to AML requirements.[98] Administrators of centralized P2P trading platforms, on the other hand, are amenable to such requirements and their incorporation into the list of obliged entities would contribute towards the goal of financial transparency, particularly in light of the fact that P2P trading constitutes a significant portion of all crypto trades.[99]

As legislators decided to focus on the intermediaries operating in the crypto ecosystem, the regulation of users failed to garner comparable attention. The matter of VC user regulation is only marginally touched upon in AMLD V. Recital 9 notes the possibility of introducing a system of registration in which individuals voluntarily self-declare as VC users.[100] In addition, the directive leaves open the possibility of including user registration (through a self-declaration form) in a legislative proposal that was meant to be published in January 2022.[101] Mindful of the fact that anonymity features draw many users to cryptocurrency in the first place, a system grounded on voluntary self-declaration (effectively ending anonymity) would probably lack any positive effect (unless it was supplemented by an incentive mechanism), and it could be more prudent to consider mandatory user registration as an alternative.

96 *Chainalysis Team*, The 2022 Crypto Crime Report, available at: https://go.chainalysis.com/2022-Crypto-Crime-Report.html (22/3/2023), pp. 12, 14.
97 Ibid., p. 115.
98 *OECD*, The Tokenisation of Assets and Potential Implications for Financial Markets, available at: https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm (22/3/2023), p. 30.
99 *FATF*, Second 12-Month review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html (22/3/2023), pp. 25–26 this is the case for Bitcoin; in fact, more than half of all Bitcoin transactions take place without an intermediary.
100 AMLD V, Recital 9 of the Preamble.
101 Ibid., para. 41, to the author's knowledge, this publication never took place.

Lastly, it is worth touching upon the topic of obliged entity registration. In the proposal for AMLD V, the legislators empowered the member states to choose between a system of licensing and registration for VC intermediaries.[102] However, in its final version, AMLD V was scaled-down to include the less intrusive of the two regimes, and states now ensure that all persons, falling under the category of VC obliged entities, are registered with the competent national authorities.[103] Accordingly, a question that emerges is whether licensing VC intermediaries would have been more beneficial for the purpose of exerting greater control over the sector and reducing crypto money laundering risk.

IV. Soft Law to the Rescue: The FATF Approach

The FATF has been an important proliferator of AML standards for well over thirty years. The FATF Recommendations have, despite their non-binding nature, exerted decisive influence on global and European legislation. In fact, an amendment of the FATF Recommendations usually triggers a corresponding change in the European AML framework.[104] Owing to the developments in crypto-markets and the need to adapt the Recommendations to the domain, the FATF undertook a revision of its standards in late 2018, which resulted in the adoption of brand-new terminology, i.e., the concepts of virtual asset and virtual asset service provider (hereinafter VASP).

The FATF definition of a virtual asset is quite similar to the concept of virtual currency retained by the EU in AMLD V. However, the former is broader in the sense that it encompasses all three major categories of crypto-assets, which are equally suitable for money laundering/terrorist financing purposes.[105] A virtual asset is defined in a technologically-agnostic fashion as a "digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes";[106] accordingly, this definition encapsulates not only cryptocurrencies but also investment and utility tokens. Moreover, the FATF has defined a VASP as a natural or legal person that:

> as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i) exchange between virtual assets and fiat currencies; ii) exchange between one or more forms of virtual assets; iii) transfer of virtual assets; iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.[107]

102 AMLD V Proposal, p. 37 para. 16.
103 AMLD IV, Art. 47-1.
104 *Penna*, in: Ligeti/Simonato (eds.), p. 270, the first four European AML Directives have been adopted following corresponding revisions of FATF standards.
105 *Houben/Snyers*, in: Liaw (ed.), p. 173.
106 *FATF*, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation 2012-2023, p. 135.
107 Ibid., p. 133.

According to the definition, a corporate or individual that is actively involved in the provision of any of the five above-enumerated activities, and provides them to customers on a commercial basis qualifies as a VASP.[108] Importantly, in its Recommendation 15 pertaining to "new technologies", the FATF recommends the subjection of VASPs to "adequate regulation and supervision or monitoring for AML/CFT [purposes]".[109] It is also suggested that states should ensure that these entities adhere to requirements aiming to "mitigate money laundering and terrorist financing risks emerging from virtual assets".[110] Tellingly, the FATF has taken the matter of obliged entity regulation a step further than the European legislators. Instead of enumerating obliged entities, the FATF provides a wide, forward-looking definition. Indeed, the VASP concept does not only encompass fiat to crypto VCEs and custodian wallet providers, the two major intermediaries captured by the provisions of AMLD V. It is broad enough to include other crypto-market entities, e.g., crypto to crypto VCEs, bitcoin ATMs,[111] centralized P2P trading platforms[112] and providers of mixing services.[113]

In addition, the FATF standards propose that VASPs should be subject to licensing or registration requirements.[114] Again, when compared to AMLD V, it can be observed that the FATF goes a step further. It advises its members to introduce VASP registration or the more intrusive licensing regime. Furthermore, the FATF leaves it to the member states to devise the exact registration/licensing criteria. However, it recommends that the authorities should be able to examine whether the VASP is in a position to fulfil its AML obligations.[115]

Another important development refers to the extension of the so-called travel rule to virtual assets and VASPs. The travel rule is contained in FATF Recommendation 16, and it has initially applied to payment service providers (hereinafter

108 *FATF*, Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers, available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (22/3/2023), paras. 58–62.

109 Ibid., Interpretative Note to Rec. 15, pp. 76–77.

110 Ibid., in essence, VASPs must adhere to the same anti-money laundering/countering the financing of terrorism requirements imposed on traditional obliged entities, outlined in recommendations 10 to 21.

111 Ibid., para. 71.

112 Ibid., paras. 67–70 and 90–91, as long as a P2P trading platform has an underlying party that engages in any of the VASP activities (even if partly), it can be classified as a VASP.

113 Ibid., para. 85, the paragraph covers mixers, albeit as an added service provided by exchange platforms; nevertheless, even if the service were to be provided by an independent entity, it would qualify as a VASP, seeing that it facilitates the "transfer of virtual assets" from one wallet to another.

114 *FATF*, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation 2012-2023, p. 76, para 3, VASPs are to be registered/licensed in the jurisdiction of incorporation/where the place of business is located.

115 *FATF*, Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers, available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (22/3/2023), para. 131.

PSPs) facilitating wire transfers above a predetermined threshold.[116] PSPs are required to accompany all fund transfers with information on the payer and payee. Following FATF's augmentation of the rule, originator VASPs are now obliged to collect accurate information (e.g., full name and account number, if any) of the originator and beneficiary of a virtual asset transfer and provide this information to the beneficiary VASP and, upon request, the appropriate authorities.[117] In a similar fashion, beneficiary VASPs are obliged to collect and store identical data and cooperate with the authorities. Importantly, in order to ensure data completeness, the beneficiary VASP should be in a position to detect whether the information on the originator and beneficiary, received from the originator VASP, is missing or incomplete and request remediation.[118]

The core objective of the modified travel rule is to inhibit criminals from having unfettered access to electronic transfers of virtual assets and detect instances of misuse.[119] The travel rule supports the ability of FIUs to track movements of virtual assets and follow the transaction trail to the originator. Importantly, the travel rule has been incorporated into the existing European legal framework, albeit without the inclusion of VASPs or virtual assets.[120]

D. European Crypto AML Regulation: Quo Vadis?

In an effort to enhance the European AML/CFT regime, the European Commission proposed the adoption of several legislative acts on 20 July 2021. These acts include: 1) the proposal for an AMLD VI,[121] 2) proposal for an AML Regulation,[122] and 3) proposal for a revision of Regulation (EU) 2015/847 on transfers of funds.[123] These three proposals are to be read jointly and constitute the "EU single rulebook

116 *FATF*, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation 2012-2023. Recommendation 16 (p. 17–18) details the travel rule. More details are provided in the interpretative note to Rec. 16 (p. 80).

117 Ibid., p. 77, para 7-b.

118 Ibid., p. 81, para. 19.

119 *FATF*, Updated Guidance for a Risk-based Approach: Virtual Assets and Virtual Asset Service Providers, available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (22/3/2023), para. 175.

120 Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, OJ L 141 of 5/6/2015, Art. 2-1.

121 *European Commission*, Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849 (hereinafter AMLD VI), COM/2021/423 final.

122 *European Commission*, Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (hereinafter AML Regulation), COM/2021/420 final.

123 *European Commission*, Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast) (hereinafter Regulation on the traceability of crypto-assets), COM/2021/422 final.

on AML/CFT"[124] (hereinafter EU rulebook). The EU rulebook contains valuable insights regarding the potential way forward for EU cryptocurrency AML regulation.

There are two major changes proposed in the EU rulebook. Firstly, it expands the scope of the European AML/CFT framework to include the "crypto-asset service provider" (hereinafter CASP) and "crypto-asset" concepts,[125] which correspond to FATF's definitions of "VASP" and "virtual asset".[126] This development effectively remedies two major flaws of AMLD V, i.e., its narrow focus on crypto to fiat VCEs/custodian wallet providers as obliged entities and its restricted (crypto-centric) definition of virtual currency.

Secondly, the EU rulebook proposes the adoption of the updated FATF travel rule. Similar to their VASP counterparts, originator CASPs would be required to collect, store, and verify the information on the originator and collect basic information on the beneficiary. This information is submitted to the beneficiary CASP before or at the moment of the transfer.[127] The beneficiary CASP checks the completeness of the data before making the crypto-assets available to the beneficiary. In case of missing or incomplete data, the beneficiary CASP may reject the transfer or ask the originator CASP to submit the missing information within a deadline.[128] The originator and beneficiary CASPs are obliged to cooperate with the authorities and report suspicious activity.[129] Obliging CASPs to collect, record and share accurate and complete originator/beneficiary data and report suspicious crypto-asset transfers provides invaluable support and information to FIUs and other law enforcement agencies responsible for investigating financial crime. Ultimately, tracing suspicious transactions back to the originator is what enables authorities to disperse complex layering structures utilized by crypto money launders and establish the genuine source of (illicit) crypto-assets.

Having examined the regulatory developments set forth by the FATF and mirrored through the EU rulebook, it can be concluded that there are multiple ways to proceed forward to develop the existing European AML regime. Firstly, it would be possible to carry on with the intermediary-based approach, focused on the imposition of AML requirements on the gatekeepers of the crypto-markets. This would necessitate the expansion of the list of obliged entities to include actors other than fiat to crypto VCEs and custodian wallet providers, the primary obliged entities under the existing framework. This could be achieved by enumerating the obliged entities or by way of introducing new terminology, as was done by the FATF. Recent legislative proposals clearly indicate an inclination towards the second approach. The

124 AMLD VI, p. 2 of the Explanatory Memorandum.
125 AML Regulation, para. 11 of the Preamble. The precise definition of the terms "CASP" and "crypto asset" can be found in: *European Commission*, Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final, Art. 3-1(8), 3-1(9) and 3-1(2).
126 Regulation on the traceability of crypto-assets, p. 4 of the Explanatory Memorandum.
127 Ibid., Recital 31 of the Preamble.
128 Ibid., Art. 17-1, para 2.
129 Ibid., Art 18.

proposed CASP definition included in the EU rulebook, corresponding to FATF's VASP, can be seen as a forward-looking and future-proof solution. The definition is structured wide enough to encompass not only the existing crypto market participants that are beyond the reach of AMLD V (e.g., tumblers) but also any other new business model that might emerge in the future.

In addition, the introduction of a registration and licensing regime for obliged entities (CASPs) is an amendment worth considering from the perspective of increased regulatory oversight and money laundering risk minimization. In this regard, the provisions of the proposed Regulation on Markets in Crypto-assets (hereinafter MiCA Regulation) prove highly instructive. The MiCA Regulation proposes a regime in which competent national authorities grant licenses for the provision of crypto-asset services. The MiCA regulation indicates that only authorized legal persons with a registered office in the EU may provide crypto-asset services.[130] As a consequence, natural persons are barred from applying for authorization and are unable to provide crypto-asset services. This approach differs from that of the FATF, which foresees the possibility of natural and legal persons operating as a VASP.[131] Importantly, the reduction of CASPs to legal entities goes against the letter of the proposed EU rulebook.[132] Leaving aside the aforementioned discrepancy, the MiCA Regulation proposes a detailed regime for authorization. The process begins with the submission of an application coupled with additional data and documentation.[133] Importantly, proof that the managers possess sufficient knowledge, skills experience as well as a non-existent criminal record is requested.[134] Following authorization, the name of the licensed CASP is included in a register maintained by the European Securities and Markets Authority.[135]

On the other hand, a model for cryptocurrency user registration has not been considered by recent legislative proposals. To reiterate, it is highly unlikely that a system based on self-declaration would yield any meaningful outcome. Hence, there may be merit in opting for mandatory user registration. If such an intrusive system were to be considered, legislators would need to carefully deliberate a number of topics, such as whether all crypto users should be subject to registration requirements, the type of data that should be provided, whether the registration obligation should be triggered *ex-ante* or following acquisition of crypto, whether user registers should be kept at a national or European level and so on.

130 *European Commission*, Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final (hereinafter MiCA Regulation), Art. 53-1.

131 Refer to: Heading IV "Soft Law to the Rescue: The FATF Approach".

132 Regulation on the traceability of crypto-assets, p. 4 of the Explanatory Memorandum, indicating that "the list of [..] crypto-asset services providers (CASPs) […] encompasses the virtual asset services providers (VASPs) identified as such by the FATF […]".

133 MiCA Regulation, Art. 54-2(a) to (e), requiring the applicant to provide its name and denomination, articles of association, description of governance arrangements and list of services it intends to provide.

134 Ibid., Art. 54-2(f) and (g).

135 Ibid., Art. 57-1.

Furthermore, it is crucial for EU legislators to take a position on the matter of privacy coins. As privacy coins rely on technology that clouds sensitive transaction details, they hamper user traceability while providing a level of anonymity that is particularly suitable for the facilitation of clandestine transactions. A possible solution might be borrowed from the newly proposed approach for bearer share regulation. Bearer shares can be observed as a non-virtual counterpart of privacy coins. They are physical certificates that grant the holder ownership interest in a legal entity. As bearer shares represent unregistered securities the identity of the holder is never recorded and there is no register to track the transfer of ownership.[136] Money launderers have been known to abuse this instrument and the European Parliament has described it as a "very useful tool for creating international schemes for money laundering".[137] Unsurprisingly, the EU rulebook has taken an antagonistic stance and has prohibited companies from issuing bearer shares.[138] Accordingly, one possible regulatory approach for privacy coins would be the imposition of an outright ban on their issuance, acquisition and trade.[139] This prohibition could be supplemented with criminal sanctions, e.g., incarceration, monetary fines or other penalties, which might aid in deterring issuance/acquisition.

It can be clearly seen that all the existing regulations on cryptocurrencies mechanically expand the AML obligations originally intended for traditional financial institutions to the entities operating in the cryptocurrency domain. Essentially, the intermediaries of the crypto ecosystem are treated as though they were credit and financial institutions and there is hardly any acknowledgement of their particularities and the technological specificities of cryptocurrency, e.g., blockchain/distributed ledger technology. What is more, in spite of efforts to regulate the key actors of the crypto ecosystem by means of imposing AML obligations, users have the ability to bypass crypto gatekeepers by transacting on a pure P2P basis or through OTC trading, thereby circumventing the full scope of KYC measures that would normally apply.[140] In fact, a recent study commissioned by the FATF indicates that a significant portion of all bitcoin transactions take place on a disintermediated basis, i.e., in the absence of an entity obliged to implement AML measures.[141] Importantly, in case of a future increase in the number of disintermediated trades- the intermediary-

136 *OECD*, Behind the Corporate Veil: Using Corporate Entities for Illicit Purposes, available at: https://doi.org/10.1787/9789264195608-en (22/3/2023), p. 30.

137 *Clarke*, in: Birkomose et al. (eds.), para. 10. 04.

138 AML Regulation, Art. 58-3.

139 Allegedly, a legislative draft has been submitted for discussion by a Czech EU delegation proposing to prohibit CASPs as well as financial and credit institutions from safekeeping privacy coins, see: *Coindesk*, Privacy-Enhancing Crypto Coins Could Be Banned Under Leaked EU Plans, available at: https://www.coindesk.com/policy/2022/11/15/privacy-enhancing-crypto-coins-could-be-banned-under-leaked-eu-plans/ (22/3/2023).

140 *Europol*, *Europol*, Cryptocurrencies: Tracing the Evolution of Criminal Finances, available at: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances (22/3/2023), p. 9.

141 Four of the six blockchain analytics companies that were employed for the study have found that 60% of all bitcoin transactions, in the period from 2016 to 2020, took place in the absence of a VASP, see FATF, Second 12-Month review of the Revised FATF Stan-

based approach would be rendered ineffective. The solution to this predicament could lie in acknowledging the public nature of blockchain. To reiterate, verified transactions in bitcoin (and similarly structured altcoins) are stored in blocks of data shared between the entire network. Importantly, such a design provides absolute transparency, where all transactions become traceable and visible to system participants, following verification.

To supplement the intermediary-based approach of cryptocurrency AML regulation, the EU (or its member states) could support the adoption and finance the development[142] of blockchain analysis tools. These tools can be applied by national law enforcement agencies and FIUs as well as CASPs to detect illicit crypto transactions and deanonymize wrongdoers. One example of such a tool is BitIodine, an automated software solution that processes blockchain data and applies heuristics for clustering purposes, i.e., the creation of groupings of crypto addresses.[143] The system incorporates a set of "scrapers" that search the web and collect publicly available off-chain user information (e.g., stored on web forums) used to label users and trace transactions within the digital domain.[144] Importantly, BitIodine has found real-world use and has assisted the FBI in identifying a cryptocurrency transaction made for the benefit of a contract killer.[145] Similarly, the forensic software solution Chainalysis Reactor has been adopted by the Bank of New York Mellon Corporation as well as Canadian law enforcement agencies.[146] Chainalysis Reactor works by linking crypto transactions, i.e., user wallets, to real-world entities. Much like BitIodine's software, it utilizes different heuristics to generate data clusters and identify controlling entities behind them.[147] Finally, blockchain analytics tools developed by the company Elliptic were used to promptly identify a wallet used by the ransomware group DarkSide.[148] The wallet was used to collect payments obtained from victims, including 75 bitcoins received from Colonial Pipeline following a cy-

dards on Virtual Assets and Virtual Asset Service Providers, available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html (22/3/2023), pp. 25–26.

142 *ZDNET*, IRS offers grants for software to trace privacy-focused cryptocurrency trades, available at: https://www.zdnet.com/article/irs-offers-grants-to-contractors-able-to-trace-cryptocurrency-transactions-across-the-blockchain/ (22/3/2023), reporting how the IRS has been offering grants of up to USD 625 000 for contractors that develop tech solutions for tracking privacy coins.

143 *Spagnuolo et al.*, FCDS 2014, pp. 460–461.

144 Ibid.

145 Ibid., p. 9.

146 *Chainalysis Team*, BNY Mellon To Integrate Chainalysis Product Suite for Cryptocurrency Compliance, available at: https://blog.chainalysis.com/reports/chainalysis-bny-mellon-announcement/ (22/3/2023). See also: *Commission of Inquiry into Money Laundering in British Columbia*, Proceedings at Hearing of November 24, 2020, available at: https://cullencommission.ca/data/transcripts/ (22/3/2023), pp. 126–127.

147 Ibid., pp. 129–130 and 132.

148 *Elliptic*, Elliptic Follows the Bitcoin Ransoms Paid by Colonial Pipeline and Other DarkSide Ransomware Victims, available at: https://www.elliptic.co/blog/elliptic-follows-bitcoin-ransoms-paid-by-darkside-ransomware-victims (22/3/2023).

berattack on their operating system. As a result of Elliptic's efforts, crypto market actors are able to track the movement of crypto stored in DarkSide's tainted wallet.

Importantly, the number of third-party vendors providing blockchain analysis solutions appears to be increasing.[149] As these tools demonstrate the potential to facilitate and catalyze the identification of dishonest crypto users, obliged entities could utilize them to, e.g., identify the source of funds, detect and report suspicious transaction activity, screen user wallets and so on. Moreover, as real-world examples have shown, FIUs and law enforcement agencies can rely on blockchain analysis to support their investigations. Accordingly, the introduction and development of blockchain analysis software solutions should be promoted to augment the regulatory pressure facilitated through the intermediary-based approach of AML regulation.

E. Conclusion

This study has provided an analysis of the concept of cryptocurrency money laundering and has examined its regulation in the EU AML framework. It has reached the conclusion that the present regime, centered around the AMLD V, is not sustainable from the perspective of efficient and comprehensive regulation.

To rectify these shortcomings, this paper has advocated for a two-pronged approach. It has proposed, in the first step, the revision of AMLD V provisions and the incorporation of solutions that mimic those of the FATF in terms of regulating the key actors of the crypto markets. Additionally, the present framework could be amended to include mandatory user registration and the licensing of CASPs, as proposed by the European Commission. To reiterate, on the one hand mandatory user registration would enable national authorities to collect (and subsequently exchange with one another) vital information concerning cryptocurrency users, thereby ending (to an extent) user anonymity. On the other hand, CASP licensing would grant national authorities an active role in shaping the market of crypto-service providers; whereby entities failing to demonstrate comprehensive internal governance, qualified and reputable management etc. would be barred from engaging in service provision. Importantly, both regulatory adjustments could lead to greater financial transparency and improved governance.

Secondly, the intermediary-based approach of money laundering regulation should be paired with a method centered around the exploitation of transaction transparency, i.e., blockchain analysis. Indeed, the public nature of blockchain technology behind Bitcoin and analogous altcoins could be employed to surpass the inherent limitations of the intermediary-based approach. The introduction of blockchain analytics into the arsenal of instruments applied by national law enforcement

149 *StartupStash*, Top 32 Blockchain Analysis Tools, available at: https://startupstash.com/blockchain-analysis-tools/ (22/3/2023), the webpage includes a list of 32 most popular vendors providing blockchain analysis software.

authorities, FIUs and AML obliged entities would constitute a desirable development from the perspective of preventing and detecting money laundering.

The advent of crypto money laundering has presented itself as a complex challenge for European legislators. Owing to the fast-paced development of the ecosystem and the growing interconnectedness between cryptocurrency and the traditional financial sector, innovative and forward-looking solutions are a *conditio sine qua non* for preventing the instrumentalization of crypto for money laundering. As cryptocurrency holds the promise of an accessible, expeditious and economical transaction system, it is imperative to disperse the criminal label attached to it and work towards improving credibility through calculated regulation.

Bibliography

ANDROULAKI, ELLI; KARAME, GHASSAN O; ROESCHLIN, MARC; SCHERER, TOBIAS; CAPKUN, SRDJAN, *Evaluating User Privacy in Bitcoin*, in: Sadeghi, Ahmad-Resza (eds.), Financial Cryptography and Data Security, Lecture Notes in Computer Science, Vol. 7859, Berlin–Heidelberg, 2013, pp. 34–51

ARSLANIAN, HENRI, *The Book of Crypto: The Complete Guide to Understanding Bitcoin, Cryptocurrencies and Digital Assets*, 1st ed., Cham, 2022

AZANI, EITAN; LIV, NADINE, *Jihadists' Use of Virtual Currency*, International Institute for Counter Terrorism, 2018, available at: http://www.jstor.org/stable/resrep17688 (26/4/2023)

BAZAN-PALOMINO, WALTER, *Bitcoin and Its Offspring: A Volatility Risk Approach*, in: Pichl, Lukas; Eom, Cheoljun; Scalas, Enrico; Kaizoji, Taisei, Advanced Studies of Financial Technologies and Cryptocurrency Markets, 1st ed., Singapore, 2020, pp. 233–256

CAMPBELL-VERDUYN, MALCOLM, *Bitcoin, crypto-coins, and global anti-money laundering governance*, Crime Law and Social Change, 2018, Vol. 69, Issue 2, pp. 283–305

CHOHAN, USMAN W., *Accessing the Differences in Bitcoin and other Cryptocurrency Legality Across National Jurisdictions*, 26/2/2022, SSRN, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3042248 (22/3/2023)

CLARKE, BLANAID, *Unmasking Shareholders and Directors to Prevent the Abuse of Companies,* in: Birkmose, Hanne S.; Neville, Mette; Sorensen, Karsten Engsig (eds.), Abuse of Companies, 1st. ed., 2019, Chapter 10

HAFFKE, LARS; FROMBERGER, MATHIAS; ZIMMERMANN, PATRICK, *Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them*, Journal of Banking Regulation, 2020, Vol. 21, Issue 2, pp. 125–138

HENCIC, ANDREW; GOURIEROUX, CHRISTIAN, *Noncausal Autoregressive Model in Application to Bitcoin/USD Exchange Rates*, in: Huynh, Van-Nam; Kreinovich, Vladik; Sriboonchitta, Songsak; Suriya, Komsan(eds.), Econometrics of Risk, 1st ed., Berlin, 2015, pp. 17–41

HETZEL, J. FLORIAN, *The Act of Cleaning Illegal Profits: What we Know and Don't Know about Money Laundering*, in: Reichel, Philip; Randa, Ryan (eds.), Transnational Crime and Global Security, 1st ed., Connecticut, 2018, pp. 115–139

HOUBEN, ROBBY; SNYERS, ALEXANDER, *Cryptoassets and financial crime: a European Union perspective*, in: Liaw, Thomas K. (ed.), The Routledge Handbook of FinTech, 1st ed., New York, 2021, pp. 163–191

IRWIN, ANGELA S.M.; REYNOLDS, PERRI, *Tracking digital footprints: anonymity within the bitcoin systems*, Journal of Money Laundering Control, 2017, Vol. 20, Issue 2; pp. 172–189

JUDMAYER, ALJOSHA; STIFTER, NICHOLAS; KROMBHOLZ, KATHARINA; WEIPPL, EDGAR, *Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies and Their Consensus Mechanism*, 1st ed., New York, 2017

JUHÁSZ, PÉTER L.; STÉGER, JÓZSEF; KONDOR, DANIEL, VATTAY, GÁBOR, *A Bayesian approach to identify Bitcoin users*, Public Library of Science, 2018, available at: https://doi.org/10.1371/journal.pone.0207000 (22/3/2023)

KARAME, GHASSAN; ANDROULAKI, ELLI, *Bitcoin and Blockchain Security*, 1st ed., Boston, 2016

KEPLI, MOHD; ZULHUDA, SONNY, *Cryptocurrencies and Anti-money Laundering Laws: The need for an Integrated Approach*, in: Oseni, Umar A.; Hassan M. Kabir; Hassan, Rusni (eds.), Emerging Issues in Islamic Finance Law and Practice in Malaysia, 1st ed., Bingley, 2019, pp. 247–265

KERMITSIS, EMMANOUIL et al., *Dark Web Markets*, in: Aghar, Babak; Gercke, Marco; Vrochidis, Stefanos; Gibson, Helen, Dark Web Investigation, 1st ed., Berlin, 2021, p. 85–119

KETHINENI; SESHA, *Dark Web/Deep Web*, in: Reichel, Philip (ed.), Global Crime: An Encyclopedia of Cyber Theft, Weapons Sales, and other illegal activities, 1st ed., Santa Barbara, 2019, pp. 159–162

KIZZA, JOSEPH MIGA, *Guide to Computer Network Security*, 5th ed., Berlin, 2020

KYLES, DIANNA L., *Centralised Control over Decentralised Structures: AML and CTF Regulation of Blockchains and Distributed Ledgers*, in: Goldbarsht, Doron; De Koker, Louis (eds.), Financial Technology and the Law: Combating Financial Crime, 1st ed., Berlin, 2022, pp. 121–151

MADINGER, JOHN, *Money Laundering: A Guide for Criminal Investigations*, 3rd ed., London, 2012

MADSEN, FRANK G., *Transnational Organized Crime*, 1st ed., New York, 2009.

PENNA, MARC, *The 'Pre-investigative' Role of Financial Intelligence Units in Recovering Assets*, in: Ligeti, Katalin; Simonato, Michele (eds.), Chasing Criminal Money: Challenges and Perspectives on Asset Recovery in the EU, 1st ed., Oxford, 2017, pp. 269–286

SATHYA, AR; ELNGAR, AHMED A., *Bitcoin: A P2P Digital Currency*, in: Panda, Sandeep Kumar; Elngar, Ahmed A.; Balas, Valentina Emilia; Kayed, Mohammed (eds.), Internet of Everything: Bitcoin and Blockchain: History and Current Applications, 1st ed., London, 2020. pp. 1–23

REID, FERGAL; HARRIGAN, MARTIN, *An Analysis of Anonymity in the Bitcoin System*, in: Altshuler, Yaniv; Elovici, Yuval; Cremers, Armin B.; Aharony, Nadav; Pentland, Alex (eds.), Security and Privacy in Social Networks, 1st ed., New York, 2013, pp. 197–225

RICHARD, JAMES R., *Transnatihonal Criminal Organizations, Cybercrime and Money Laundering*, 1st ed., London, 1999

ROSSEL, LUCIA; UNGER, BRIGITTE; BATCHELOR, JASON; VAN KONIGSFELD, JAN, *The Implications of Making Tax Crimes a Predicate Crime for Money Laundering in the EU: Building a Legal Dataset of Tax Crimes and Money Laundering in the European Union*, in Unger, Brigitte; Rossel, Lucia; Ferwerda, Joras (eds.), Combating Fiscal Fraud and Empowering Regulators, 1st ed., Oxford, 2021, pp. 236–272

SCHOTT, PAUL ALLAN, *Reference Guide to Anti-money Laundering and Combating the Financing of Terrorism*, 2nd ed., Washington, 2006

SIMSER, JEFFREY, *Bitcoin and modern alchemy: in code we trust*, Journal of Financial Crime, 2015, Vol. 22, Issue 2, pp. 156–169

SMYCZEK, SLAWOMIR, *Consumer Attitudes to the Phenomenon of Money Laundering*, in: Petr, Chadraba G.; Springer, Reiner (eds.), Business Strategies for Economies in Transition: Book of Readings on CEE Counties, 1st ed., Cambridge, 2008, pp. 488–522

SPAGNUOLO, MICHELLE et al., *BitIodine: Extracting Intelligence from the Bitcoin Network*, in: Christin, Nicholas; Safavi-Naini (eds.), Financial Cryptography and Data Security, 2014, Lecture Notes in Computer Science, Vol. 8437, Berlin, Heidelberg

TEICHMANN, FABIAN MAXIMILIAN JOHANNES; FALKER, MARIE-CHRISTIN, *Money Laundering via Cryptocurrencies- potential solutions from Liechtenstein*, Journal of Money Laundering Control, 2021, Vol. 24, Issue 4, pp. 775–788

TSINGOU, ELLENI, *Money Laundering*, in: Mügge, Daniel (ed.), Europe and the Governance of Global Finance, 1st ed., Oxford, 2014, pp. 141–156

VACCA, JOHN R., *Managing Information Security*, 2nd ed., London, 2014

ZHANG, SHOUTONG, *Bitcoin and Other Blockchain Technologies: Mechanisms, Governance, and Applications*, in: Pompella, Maurizio; Matousek, Roman (eds.), The Palgrave Handbook of FinTech and Blockchain, London, 1st ed., 2021, pp. 243–259