



JULIA CASTRO LUCAS DA SILVA

**THE ANTITHESIS BETWEEN THE KYC PRACTICES TO  
COMBAT MONEY LAUNDERING AND THE  
INCREASING PRESENCE OF CRYPTOCURRENCIES**

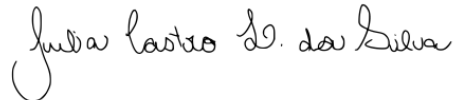
Dissertation to obtain a Master's Degree  
in Law, in the speciality of Business Law  
and Technology.

Supervisor:  
Dr. Athina Sachoulidou, Professor at NOVA School of Law

2022  
February

## **ANTI-PLAGIARISM STATEMENT**

I hereby declare that the work I present is my own work and that all my citations are correctly acknowledged. I am aware that the use of unacknowledged extraneous materials and sources constitutes a serious ethical and disciplinary offence.

A handwritten signature in black ink, reading "Julia Castro L. da Silva". The script is cursive and fluid, with the first letter of each word being capitalized and prominent.

Julia Castro Lucas da Silva

## **ACKNOWLEDGEMENTS**

This dissertation would not have been possible without the guidance and sharp feedback of Professor Athina Sachoulidou. I am grateful to her for making herself available to answer my doubts promptly and for her generosity.

I am grateful to Marco, Miriam, and Olaf for their continuous support and for believing in me.

## **STATEMENT REGARDING LENGTH OF DISSERTATION**

The body of this dissertation, including spaces and notes, occupies a total of 149.419 characters.

## **ABSTRACT**

Imposing know-your-customer requirements on obliged entities has been an important element of the strategy of the European Union for addressing money laundering. Nonetheless, know-your-customer requirements pose challenges to obliged entities, and to their customers. Additionally, know-your-customer as a concept often collides with the anonymity allowed by cryptocurrencies, which operate using blockchain technology, which does not require a central organization for functioning. Although the transactions in most blockchains are public, the users in a blockchain are only identified by their addresses and have the possibility to create an unlimited number of new addresses. The obligations imposed on cryptocurrency service providers by the 5<sup>th</sup> Anti-Money Laundering Directive do not consider all the aspects that can be misused by money launderers by means of cryptocurrencies. The European Union's Anti-Money Laundering Action Plan and the Digital Finance Strategy may lead to a significant progress in relation to the legislation in force as to addressing money laundering risks that arise from new technologies. However, these risks cannot be addressed only by focusing on know-your-customer policies. This work contributes to the ongoing debate by analysing how the current legislation addresses money laundering risks related to cryptocurrencies and how the plans of the European Union will tackle the matter.

## RESUMO

A imposição de requisitos de *know-your-customer* (“conheça seu cliente”, em português) é um elemento importante da estratégia da União Europeia para combater o branqueamento de capitais. No entanto, os requisitos relacionados a *know-your-customer* representam alguns obstáculos para as entidades obrigadas, e para seus clientes. Além disso, o conceito de *know-your-customer* com frequência vai de encontro ao anonimato permitido pelas criptomoedas, as quais funcionam utilizando tecnologia *blockchain*, que não requer uma organização central para funcionar. Embora as transações sejam públicas na maioria das *blockchains*, os usuários são identificados somente por seus endereços e têm a possibilidade de criar um número ilimitado de novos endereços. As obrigações impostas aos provedores de serviços de criptomoedas pela 5ª Diretiva Antibransqueamento de Capitais não consideram todos os aspectos que podem ser abusados por branqueadores de capitais por meio de criptomoedas. O Plano de Ação Contra o Branqueamento de Capitais da União Europeia e a Estratégia em matéria de Financiamento Digital podem gerar um avanço significativo em relação à legislação atual quanto ao tratamento de riscos de branqueamento de capitais que surgem de novas tecnologias. Entretanto, esses riscos não devem ser tratados somente com foco em normas de *know-your-customer*. Esse trabalho contribui para o debate em curso por analisar como a legislação atual aborda os riscos de branqueamento de capitais relacionados a criptomoedas e como os planos da União Europeia tratam do assunto.

## TABLE OF CONTENTS

<b>1. INTRODUCTION.....</b>	<b>1</b>
<b>2. THE EU AML FRAMEWORK.....</b>	<b>4</b>
<b>2.1. The role and influence of the FATF Recommendations .....</b>	<b>5</b>
<b>2.2. Legislation at EU level.....</b>	<b>7</b>
2.2.1. Origins of the EU AML rules .....	8
2.2.2. KYC and the role of the private sector in the AMLD.....	10
<b>3. THE ROLE OF PREVENTION IN ANTI-MONEY LAUNDERING.....</b>	<b>13</b>
<b>3.1. Challenges arising from the KYC requirements in the field of money laundering prevention.....</b>	<b>14</b>
<b>3.2. Clusters of challenges arising from KYC requirements .....</b>	<b>17</b>
<b>4. CONTROVERSIES ASSOCIATED WITH THE USE OF CRYPTOCURRENCIES .....</b>	<b>18</b>
<b>4.1. Understanding Blockchain and the origins of Cryptocurrencies.....</b>	<b>22</b>
<b>4.2. Anonymity: a key factor of the use of cryptocurrencies .....</b>	<b>25</b>
4.2.1. How anonymity can enable money laundering by means of cryptocurrencies.....	29
<b>4.3. Increased popularity of cryptocurrencies among criminals.....</b>	<b>33</b>
<b>5. THE ANTITHESIS BETWEEN KYC AS A MEANS OF PREVENTING MONEY LAUNDERING AND THE ANONYMITY AS A CORE ELEMENT OF CRYPTOCURRENCIES .....</b>	<b>37</b>
<b>5.1. AML rules ‘meet’ cryptocurrencies.....</b>	<b>37</b>
<b>5.2. EU future initiatives on AML and Cryptocurrencies .....</b>	<b>41</b>
5.2.1. The EU AML Action Plan and legislative proposals.....	42
5.2.2. Digital Finance Strategy and MICA .....	45
5.2.3. Critical appraisal of the EU plans .....	47
<b>5.3. How can AML policies address the anonymity in cryptocurrencies effectively?</b>	<b>51</b>
<b>6. CONCLUSION .....</b>	<b>55</b>
<b>7. BIBLIOGRAPHY .....</b>	<b>56</b>

## 1. INTRODUCTION

Preventing money laundering and terrorist financing has become a priority since the terrorist attack against the World Trade Center in September 2001<sup>1</sup>. To prevent terrorist attacks, the policy makers started turning their attention to entities in the private sector that act as gatekeepers for entering the financial market.<sup>2</sup> The know-your-customer guidelines (hereinafter KYC guidelines) have played a significant role in Anti-Money Laundering legislation/policies (hereinafter AML legislation/policies). However, they have also been the subject of intense criticism. KYC may be intrusive from the customer's perspective and even inefficient since experienced money launders may still employ a fake persona to launder money<sup>3</sup>. Moreover, AML strategies add high costs to the banking operations. For instance, it has been estimated that the actual cost of AML compliance across all financial firms in five European markets (France, Germany, Italy, Switzerland, and the Netherlands) amounts to US\$83.5 billion annually<sup>4</sup>. Besides, according to the same survey, conducted by Lexis Nexis, 40% of total AML costs are spent on KYC programmes<sup>5</sup>.

Besides being costly for the banks, AML policies can exclude some clients, such as refugees or people who have never had passports<sup>6</sup>. Countries regarded as high-risk jurisdictions have also expressed concerns about the impact AML guidelines may have on their economies<sup>7</sup>. For instance, during the Small States Forum 2016, the Minister of Finance and the Public Service in Jamaica has expressed concerns regarding the impact of high costs associated with compliance for correspondent banks<sup>8</sup>. He also stressed that the compliance costs are making correspondent banks apprehensive about doing

---

<sup>1</sup> Martin Gill and Geoff Taylor, 'Preventing Money Laundering or Obstructing Business? Financial Companies' Perspectives on "Know Your Customer" Procedures', *The British Journal of Criminology* 44, no. 4 (1 July 2004): 584, <https://doi.org/10.1093/bjc/azh019>.

<sup>2</sup> Michael Levi and Peter Reuter, 'Money Laundering', *Crime and Justice* 34 (1 January 2006): 310, <https://doi.org/10.1086/501508>.

<sup>3</sup> Gill and Taylor, 'Preventing Money Laundering or Obstructing Business?', 591.

<sup>4</sup> LexisNexis Risk Solutions, 'The True Cost of AML Compliance – European Survey European Edition', September 2017, 13, <https://risk.lexisnexis.com/global/en/insights-resources/research/the-true-cost-of-aml-compliance-european-survey>.

<sup>5</sup> *Ibid.*, 9.

<sup>6</sup> Gill and Taylor, 'Preventing Money Laundering or Obstructing Business?', 588.

<sup>7</sup> Audley Shaw, 'De-Risking and Remittances in the Caribbean' (Small States Forum 2016 - Towards a Resilient and Equitable Future: Opportunities for Financing and Partnerships, Washington DC, 6 October 2016), <https://caribbeanderisking.com/wp-content/uploads/2021/09/Minister-Shaw-De-risking-Speech-IMF-WB-Annual-Mtgs-6-Oct-2016.pdf>.

<sup>8</sup> *Ibid.*, 2.



businesses in high-risk territories<sup>9</sup>. That may reduce investment opportunities in the respective countries. Moreover, since many developing countries are classified as high-risk jurisdictions, such policies may increase the development gap.

At the same time, the bureaucracy that is inherent in customer due diligence creates friction both for customers and banks<sup>10</sup>. Due to the barriers to accessing traditional financial system, there is an increasing interest in alternative solutions that can make financial services more accessible<sup>11</sup>. Decentralised finance and cryptocurrencies in particular have been placed at the centre of attention<sup>12</sup>. Cryptocurrencies have been developing quickly for the last decade – with their users varying from individuals involved in lawful business to criminals profiting from the anonymity inherent in cryptocurrencies<sup>13</sup>.

At the same time, cryptocurrencies have presented a challenge for regulators worldwide – due, *inter alia*, to the possibility of using them to disguise illicit activities and to create complex money laundering structures. Criminals can take advantage of cryptocurrencies in several ways, including (but not limited to) Initial Coin Offers (ICOs)<sup>14</sup> and tumbler services<sup>15</sup>. In the case of ICOs, newly created cryptocurrencies can be sold bypassing KYC policies that are traditionally used for preventing money laundering<sup>16</sup>. Additionally, tumblers facilitate concealing of funds making their source difficult to be tracked<sup>17</sup>.

Transactions by means of cryptocurrencies do not require formal means of identification. The parties are only identified through pseudonyms. Cryptocurrencies operate using distributed ledger technology (hereinafter DLT), a type of database where data is stored across a distributed network of computers, which does not require a central

---

<sup>9</sup> Ibid.

<sup>10</sup> Stavros Gadinis and Colby Mangels, ‘Collaborative Gatekeepers’, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 11 March 2016), 34, <https://papers.ssrn.com/abstract=2746564>.

<sup>11</sup> Andrei Popescu, ‘Decentralized Finance (DEFI) - the Lego of Finance’, *Social Sciences and Education Research Review* 7, no. 1 (2020): 330.

<sup>12</sup> Ibid.

<sup>13</sup> Peter D DeVries, ‘An Analysis of Cryptocurrency, Bitcoin, and the Future’ 1, no. 2 (2016): 4.

<sup>14</sup> Raffaella Barone and Donato Masciandaro, ‘Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques’, *European Journal of Law and Economics* 47, no. 2 (1 April 2019): 241, <https://doi.org/10.1007/s10657-019-09609-6>.

<sup>15</sup> Lars Haffke, Mathias Fromberger, and Patrick Zimmermann, ‘Cryptocurrencies and Anti-Money Laundering: The Shortcomings of the Fifth AML Directive (EU) and How to Address Them’, *Journal of Banking Regulation* 21, no. 2 (1 June 2020): 129, <https://doi.org/10.1057/s41261-019-00101-4>.

<sup>16</sup> Ibid., 137.h

<sup>17</sup> Ibid., 136.

authority for functioning<sup>18</sup>. The lack of proper identification and the DLT technology are factors that permit the anonymity of cryptocurrency users. The anonymity allowed by blockchain technology is a factor that challenges the KYC guidelines. To address phenomena of this kind, the EU has amended the AML legislation in 2018<sup>19</sup>, extending AML and Counter-Terrorism financing rules to *some* virtual currency service providers<sup>20</sup>.

The 5th Anti-Money Laundering Directive (hereinafter AMLD)<sup>21</sup> has stipulated that service providers that deal with the exchange of cryptocurrencies for fiat currencies, which are government-issued currencies, and those that maintain wallet custody services shall enforce KYC requirements<sup>22</sup>. Although it is of great importance that crypto exchanges and wallets custody service providers correctly identify their customers, it is suspected that the KYC strategies adopted by the EU legislator do not reach the darkest side of those operations. This master thesis aims to delve into that assumption and to explore future steps to overcome the existing gaps and difficulties.

For instance, the AMLD fails to address tumbler services, which reduce the traceability by splitting a transaction into several transactions and distancing values from its source<sup>23</sup>. This service disguise cryptocurrencies coming from illicit means by making several transactions with that money and making it nearly untraceable<sup>24</sup>. It does not involve custody of wallets or exchange cryptocurrencies for fiat money. The fee for tumbler services is usually paid in the cryptocurrency transactions themselves. Therefore, these operators fall outside the scope of the AMLD in its current form.

The focus of this master thesis lies on the antithesis between the KYC guidelines and the use of cryptocurrencies, which allow for a higher level of user anonymity. It particularly aims to examine whether the KYC requirements can be applied to the cryptocurrency market efficiently and whether a further specification of the KYC

---

<sup>18</sup> Harish Natarajan, Solvej Krause, and Helen Gradstein, 'Distributed Ledger Technology and Blockchain', Working Paper, FinTech Note (Washington, DC: World Bank, 2017), 2, <https://doi.org/10.1596/29053>.

<sup>19</sup> 'Directive (EU) 2018/843 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 (Text with EEA Relevance)', 156 OJ L § (2018), <http://data.europa.eu/eli/dir/2018/843/oj/eng>.

<sup>20</sup> Věra Jourová, 'Strengthened EU Rules to Prevent' (European Commission, July 2018), 2.

<sup>21</sup> '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 (Text with EEA Relevance)' (2015), 849, <http://data.europa.eu/eli/dir/2015/849/2021-06-30/eng>.

<sup>22</sup> AMLD Art. 1 (3) (g) and (h).

<sup>23</sup> Haffke, Fromberger, and Zimmermann, 'Cryptocurrencies and Anti-Money Laundering', 129.

<sup>24</sup> Ibid.

requirements could prevent money laundering efficiently in the EU. To attain this goal, the main analysis is divided into four sections:

Section 2 will provide an overview of the EU AML framework that is currently in force. In Section 3, the focus will lie on the role of KYC in money-laundering prevention. Section 4 is devoted to the technological characteristics of cryptocurrencies – that analysis is of strategic importance inasmuch as the formulation of solutions for the ecosystem of cryptocurrencies presupposes understanding how the latter actually functions and detecting its specificities. Finally, Section 5 will explore whether and to what extent the current EU AML regime and the EU plans on AML and cryptocurrencies can prevent money laundering from taking place in the blockchain.

## **2. THE EU AML FRAMEWORK**

According to the Financial Action Task Force (hereinafter FATF), money laundering is defined as the processing of criminal proceeds to disguise their illegal origins<sup>25</sup>. The goal is to distance profits, which originate from illicit activities, from their origin. Money laundering gained its name in the United States around the 1920s due to criminals who would disguise illicit proceeds using self-service laundries<sup>26</sup>. Nevertheless, at that time, the use of the illegal proceeds was not seen as much of an issue as was the criminal activity itself<sup>27</sup>. The first set of rules aiming to combat money laundering was the Bank Secrecy Act 1970 (hereinafter BSA)<sup>28</sup>. The BSA introduced record-keeping and reporting obligations for financial institutions. At the time, the main concern was the War on Drugs and governments wanted to have the right means for punishing criminals using proceeds originating from drug-related activities<sup>29</sup>.

This Section provides an overview of how the EU AML framework is organized. Section 2.1 examines how the global standards established at the level of the Financial Action Task Force (hereinafter FATF) have exercised influence on the respective EU

---

<sup>25</sup> 'Money Laundering - Financial Action Task Force (FATF)', accessed 26 October 2021, <https://www.fatf-gafi.org/faq/moneylaundering/>.

<sup>26</sup> Guy Stessens, *Money Laundering: A New International Law Enforcement Model*, 1st ed. (Cambridge University Press, 2000), 82, <https://doi.org/10.1017/CBO9780511494567>.

<sup>27</sup> Wouter H. Muller, Christian Kalin, and John G. Goldsmith, eds., *Anti-Money Laundering: International Law and Practice* (Chichester, West Sussex, England ; Hoboken, N.J.: John Wiley & Sons / Henley & Partners, 2007), 3.

<sup>28</sup> Petrus C. van Duyn, Jackie H. Harvey, and Liliya Y. Gelemerova, *The Critical Handbook of Money Laundering: Policy, Analysis and Myths* (London: Palgrave Macmillan UK, 2018), 41, <https://doi.org/10.1057/978-1-137-52398-3>.

<sup>29</sup> Stessens, *Money Laundering*, 11–12.

legislation. Section 2.2 delves into the EU AML rules with a focus on the AML Directives.

## **2.1. The role and influence of the FATF Recommendations**

The FATF originated from a G7 meeting in Paris in 1989, where the countries were concerned about the need of having a worldwide organization that could set standards for combating money laundering<sup>30</sup>. The FATF 40 Recommendations were first introduced in 1990 and the text has been revised on several occasions ever since to improve its capacity to tackle money laundering and terrorist financing.

The text was first revised in 1996 to extend the application of the recommendations beyond drug-related offences and to keep up with the new techniques employed for money laundering purposes. The 9/11 events were the trigger to get terrorism activities under the radar of the FATF<sup>31</sup>. After the terrorist attack in the World Trade Center in October 2001, the FATF published/released Eight Special Recommendations (expanded to nine in 2004) with a focus on terrorist financing<sup>32</sup>. The 40 Recommendations were again revised in 2003 to address the evolution of money laundering techniques<sup>33</sup>. The text was revised last time in 2012, in order to provide governments with stronger tools for tackling financial crime and protecting the integrity of the financial system<sup>34</sup>. This revision has integrated the 9 Special Recommendations in the text of the 40 Recommendations<sup>35</sup>. Besides those bigger revisions, the 2012 text has been subject to small updates for the past few years, mostly for clarification purposes<sup>36</sup>. There have been fifteen small updates to the 2012 text; the last two updates took place in October 2021<sup>37</sup>. These two updates took place to clarify obligations of ‘Designated Non-Financial Business and Professions’, and to clarify the glossary definitions of ‘designated categories of offences’ and ‘financial group’<sup>38</sup>.

---

<sup>30</sup> ‘History of the FATF - Financial Action Task Force (FATF)’, accessed 20 November 2021, <https://www.fatf-gafi.org/about/historyofthefatf/>.

<sup>31</sup> FATF, ‘International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation’ (Paris: FATF, 2021 2012), 7, [www.fatf-gafi.org/recommendations.html](http://www.fatf-gafi.org/recommendations.html).

<sup>32</sup> ‘History of the FATF - Financial Action Task Force (FATF)’.

<sup>33</sup> Ibid.

<sup>34</sup> Ibid.

<sup>35</sup> Ibid.

<sup>36</sup> ‘The FATF Recommendations’, accessed 20 November 2021, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>.

<sup>37</sup> Ibid.

<sup>38</sup> Ibid.

According to the 2012 version of the FATF Recommendations, those should allow countries to:

‘identify the risks, and develop policies and domestic coordination; pursue money laundering, terrorist financing and the financing of proliferation; apply preventive measures for the financial sector and other designated sectors; establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures; enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and facilitate international cooperation’<sup>39</sup>.

The FATF is an international *ad hoc* body created by the G7<sup>40</sup>, which in turn is an informal body. Currently, there are thirty-nine members in the FATF, out of which thirty-seven are states, and two are regional organisations.

Although the provisions issued by FATF are called Recommendations, they go beyond being simple suggestions and can have implications beyond the borders of the thirty-seven states that are part of it<sup>41</sup>. For instance, according to Recommendation 19, the countries shall apply countermeasures to other countries if the FATF requests. Those countermeasures can include limiting the financial transactions with that country or with people from that country<sup>42</sup>. The consequences of countermeasures may cause damage to clients from non-compliant countries (e.g., inability to have a business relationship with certain financial institutions)<sup>43</sup>. Against this backdrop, scholars, such as Van Duyne *et al.*, argue that the countermeasures can even be considered sanctions<sup>44</sup>.

Considering the consequences of non-cooperation, it is questionable to what extent a group of only thirty-seven states may issue recommendations globally, and countries are expected to observe these Recommendations worldwide<sup>45</sup>. In practice, the FATF is setting standards on anti-money laundering worldwide, but at the same time

---

<sup>39</sup> FATF, ‘International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation’, 7.

<sup>40</sup> ‘History of the FATF - Financial Action Task Force (FATF)’.

<sup>41</sup> van Duyne, Harvey, and Gelemerova, *The Critical Handbook of Money Laundering*, 125.

<sup>42</sup> FATF, ‘International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation’, 86.

<sup>43</sup> van Duyne, Harvey, and Gelemerova, *The Critical Handbook of Money Laundering*, 142.

<sup>44</sup> *Ibid.*

<sup>45</sup> *Ibid.*, 159–60.

lacks transparency, accountability and democratic conduct <sup>46</sup>. According to van Duyne *et al.*<sup>47</sup>:

‘[...] the FATF is an informal club established by another informal club, the seven Heads of State, who in Paris in 1989 gave it a mandate for five years to fight money laundering. This informality matters as one of its consequences is that European laws on public information access do not apply to it. The Task Force has no public information duty and can release just as much to the public domain as it pleases. One cannot sue the FATF if it refuses access, because it is not a legal entity: legally it does not exist.’

Following FATF guidance without much criticism could entail serious consequences. For instance, international correspondent banks might be less interested in maintaining relations with countries that are labelled as high-risk jurisdictions or jurisdictions that are under increased monitoring by the FATF<sup>48</sup>. Banks have been implementing a de-risking strategy<sup>49</sup>, in which they avoid having high-risk clients even when there is no evidence of criminal activity related to those clients. Business relationships are terminated just because the compliance costs for maintaining the clients are high. Ultimately, there are countries that could be excluded from the global financial system due to the same issue.

## 2.2. Legislation at EU level

The EU AML legal framework stands on three pillars: prevention, repression, and collaboration. The prevention pillar focuses essentially on the role of the private sector imposing obligations to financial institutions and other entities of the private sector<sup>50</sup>. The AMLD currently contains the main set of rules that govern AML preventive measures in the EU. Concerning repression of money laundering, the main element of this pillar is the criminalization of money laundering<sup>51</sup>. On that note, Directive 2018/1673 of the

---

<sup>46</sup> Ibid., 315–16; Valsamis Mitsilegas and Niovi Vavoula, ‘The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law’, *Maastricht Journal of European and Comparative Law* 23, no. 2 (1 April 2016): 266, <https://doi.org/10.1177/1023263X1602300204>.

<sup>47</sup> van Duyne, Harvey, and Gelemerova, *The Critical Handbook of Money Laundering*, 54–55.

<sup>48</sup> Shaw, ‘De-Risking and Remittances in the Caribbean’.

<sup>49</sup> Douglas W. Arner et al., ‘The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities’, *European Business Organization Law Review* 20, no. 1 (1 March 2019): 58, <https://doi.org/10.1007/s40804-019-00135-1>; van Duyne, Harvey, and Gelemerova, *The Critical Handbook of Money Laundering*, 274–75; Shaw, ‘De-Risking and Remittances in the Caribbean’.

<sup>50</sup> Mitsilegas and Vavoula, ‘The Evolving EU Anti-Money Laundering Regime’, 262.

<sup>51</sup> Ibid.

European Parliament and of the Council sets minimum standards for criminal offenses in the subject of money laundering<sup>52</sup>. Finally, the pillar of collaboration, is centered on cooperation among Financial Intelligence Units (hereinafter FIUs)<sup>53</sup>. FIUs are institutions that receive and analyse suspicious transaction reports, sharing the results of the analysis with law enforcement when and where necessary<sup>54</sup>. The function of FIUs is regulated in the AMLD<sup>55</sup>. Additionally, there are Regulations in the EU framework which aim at establishing a collaborative system among Member States<sup>56</sup>.

The following subsections will focus on the origins of the AMLD and on specific provisions of the AMLD which will be important for the analysis of the main topic of this work.

### **2.2.1. Origins of the EU AML rules**

Since 1991, the European Parliament and Council have been publishing updated AML Directives. The 1<sup>st</sup> AMLD<sup>57</sup> was issued by the Council of the European Communities, and it was updated in 2001 by the 2<sup>nd</sup> AMLD<sup>58</sup>. In 2005, the 3<sup>rd</sup> AMLD<sup>59</sup> replaced the 1<sup>st</sup> AMLD. The AMLD currently in force is the 4<sup>th</sup> AMLD<sup>60</sup>, which was

---

<sup>52</sup> Although sometimes this Directive is referred to as the 6AMLD, this nomenclature does not seem appropriate as Directive 2018/1673 is focused on criminal measures, while AMLDs are all mainly focused on prevention.

<sup>53</sup> Mitsilegas and Vavoula, 'The Evolving EU Anti-Money Laundering Regime', 262.

<sup>54</sup> Foivi Mouzakiti, 'Cooperation between Financial Intelligence Units in the European Union: Stuck in the Middle between the General Data Protection Regulation and the Police Data Protection Directive', *New Journal of European Criminal Law* 11, no. 3 (September 2020): 353, <https://doi.org/10.1177/2032284420943303>.

<sup>55</sup> AMLD Arts. 32 to 38.

<sup>56</sup> Some examples of regulations that establish collaborations and information exchange mechanisms to aid the prevention and apprehension of money laundering are: Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds; Regulation (EU) 2018/1805 of the European Parliament and of the Council on the mutual recognition of freezing orders and confiscation orders; Regulation (EU) 2018/1672 of the European Parliament and of the Council on controls on cash entering or leaving the Union; Regulation (EU) 2019/880 of the European Parliament and of the Council on the introduction and the import of cultural goods.

<sup>57</sup> 'Council Directive 91/308/EEC of 10 June 1991 on Prevention of the Use of the Financial System for the Purpose of Money Laundering', 166 OJ L § (1991), <http://data.europa.eu/eli/dir/1991/308/oj/eng>.

<sup>58</sup> '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 - Commission Declaration', 344 OJ L § (2001), <http://data.europa.eu/eli/dir/2001/97/oj/eng>.

<sup>59</sup> 'Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing (Text with EEA Relevance)', 309 OJ L § (2005), <http://data.europa.eu/eli/dir/2005/60/oj/eng>.

<sup>60</sup> '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 (Text with EEA Relevance)', 141 OJ L § (2015), <http://data.europa.eu/eli/dir/2015/849/oj/eng>.

adopted in 2015 and was updated by the 5<sup>th</sup> AMLD<sup>61</sup> in 2018. The updates of the AML framework are deemed necessary in order to address the transformations in the financial system, allowing for more efficiency in the fight against Money Laundering<sup>62</sup>. Besides this, the revisions of the AMLD also serve to make the legislation more cohesive with the FATF Recommendations<sup>63</sup>.

The EU AMLDs have been strongly linked to the updates in the FATF Recommendations. Recital 4 of the 4<sup>th</sup> AMLD indicates that the EU legal acts should be aligned to the FATF recommendations. As mentioned above (see Section 2.1), the FATF 40 Recommendations are issued by a small group of countries and do not originate from a proper democratic process<sup>64</sup>. This is contrasting with the EU decision-making process, which is founded on a representative democracy<sup>65</sup>. In the EU, the European Parliament and the Council exercise legislative functions jointly<sup>66</sup>. The European Parliament members are directly elected by the European citizens<sup>67</sup>. Meanwhile, the Council of the European Union is formed by a representative at ministerial level of each Member State<sup>68</sup>. Once a Directive is issued by the European Parliament and the Council, it needs to be transposed to the national laws of the Member States of the EU. Therefore, while the decision-making process in the EU is legitimated by its citizens, represented in the European Parliament, and by the governments of the Member States, represented in the Council, the FATF Recommendations do not have similar legitimacy in its origins. Yet, the Recommendations and its revisions have been reproduced in the 4<sup>th</sup> AMLD and legitimized through the EU decision process<sup>69</sup>.

---

<sup>61</sup> Directive (EU) 2018/843 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 (Text with EEA relevance).

<sup>62</sup> Patrícia Godinho Silva, 'Recent Developments in EU Legislation on Anti-Money Laundering and Terrorist Financing', *New Journal of European Criminal Law* 10, no. 1 (March 2019): 4, <https://doi.org/10.1177/2032284419840442>.

<sup>63</sup> Mitsilegas and Vavoula, 'The Evolving EU Anti-Money Laundering Regime', 264.

<sup>64</sup> van Duyne, Harvey, and Gelemerova, *The Critical Handbook of Money Laundering*, 315–16.

<sup>65</sup> Treaty on the European Union, Art. 10 (1).

<sup>66</sup> Treaty on the European Union, Art. 14 (1) and Art. 16 (1).

<sup>67</sup> Treaty on the European Union, Art. 14 (3).

<sup>68</sup> Treaty on the European Union, Art. 16 (2).

<sup>69</sup> Mitsilegas and Vavoula, 'The Evolving EU Anti-Money Laundering Regime', 266.



### 2.2.2. KYC and the role of the private sector in the AMLD

The private sector is of central importance for the prevention of money laundering<sup>70</sup>. It is expected that that key players of the private sector (i.e., entities that act as gatekeepers for the financial system) collaborate with the state providing information on suspicious activity that can be an indication of money laundering<sup>71</sup>. Nonetheless, these entities need to know their clients to be able to identify patterns that can indicate suspicious activities<sup>72</sup>. This section centres on the role of the private sector in the AMLD.

The EU Anti-Money Laundering Directive turns efforts to a specific set of institutions called obliged entities. The list of obliged entities includes institutions engaged in certain business activities that represent a higher risk of being misused for money laundering<sup>73</sup>. Those entities are regarded as gatekeepers and it is expected that those agents will collaborate to preserve their reputation and to avoid sanctions imposed by the law<sup>74</sup>. Thus, the European Parliament and Council have imposed certain duties to obliged entities, such as reporting suspicious transactions<sup>75</sup> and preparing a risk assessment<sup>76</sup>.

Among the responsibilities of the obliged entities is Customer Due Diligence (hereinafter CDD)<sup>77</sup>. CDD is part of the KYC principle. According to Cox, “KYC is essentially the work conducted by a firm to undertake background checks on clients and customers to enable the firm both to obtain and confirm additional information regarding its customers”<sup>78</sup>. To be successful, KYC should not rely only on the information and documentation provided by the client<sup>79</sup>. The institutions conducting KYC need to inspect the information in a critical way<sup>80</sup>. Besides being an essential part of AML, KYC is also crucial so that banks can adjust the products offered to the profile of each client<sup>81</sup>.

---

<sup>70</sup> Ibid., 273.

<sup>71</sup> Gadinis and Mangels, ‘Collaborative Gatekeepers’, 30.

<sup>72</sup> Ibid., 33.

<sup>73</sup> Stessens, *Money Laundering*, 133.

<sup>74</sup> Gadinis and Mangels, ‘Collaborative Gatekeepers’, 3.

<sup>75</sup> AMLD Art. 31 (1) (a).

<sup>76</sup> AMLD Art. 8 (1).

<sup>77</sup> AMLD Art. 11.

<sup>78</sup> Dennis Cox, *Handbook of Anti-Money Laundering* (Chichester, West Sussex, United Kingdom: Wiley, 2014), 169.

<sup>79</sup> Ibid., 168.

<sup>80</sup> Ibid., 170.

<sup>81</sup> Ibid.

Through KYC, institutions should understand customers' source of funds and the purpose of the transactions conducted in that business relationship<sup>82</sup>.

Currently, in the EU, the AMLD prohibits Member States from allowing their financial institutions to open new anonymous accounts, and it also imposes a deadline for Member States to do CDD on existing anonymous accounts<sup>83</sup>. The Directive also states that the Member States should, through their national law, require that obliged entities conduct CDD on their clients<sup>84</sup>. Among other situations, the financial institutions should perform CDD *at the beginning of the financial relationship*. That obligation is of central importance since this stage, namely the beginning of a financial relationship, seems to be the most important for identifying criminal proceeds trying to enter the financial system<sup>85</sup>.

The Directive determines that the CDD process should include identification and verification of the identity of the customer<sup>86</sup>, identification of the beneficial owner of an account<sup>87</sup>, assessment of the purpose of the business relationship<sup>88</sup>, ensuring that the activity in the account is coherent with the information collected on the customer, and ensuring that the information on the client is updated<sup>89</sup>. The CDD process may also be enhanced<sup>90</sup> or simplified<sup>91</sup> depending on risk factors.

According to the AMLD, the Member States are also obliged to establish FIUs<sup>92</sup>. These entities are responsible for receiving and analysing suspicious transactions reported by obliged entities and other information relevant to money laundering<sup>93</sup>. The obliged entities should also provide information to the FIU upon request<sup>94</sup>. FIUs should be independent and autonomous bodies<sup>95</sup>. The EU does not prescribe a specific form to the FIUs, and Member States have opted for different types of FIUs, that *Mitsilegas* categorizes in four models: independent FIUs, administrative FIUs, police FIUs, and

---

<sup>82</sup> Ibid.

<sup>83</sup> AMLD Art. 10 (1).

<sup>84</sup> AMLD Art. 11.

<sup>85</sup> Stessens, *Money Laundering*, 146.

<sup>86</sup> AMLD Art. 13 (1) (a).

<sup>87</sup> AMLD Art. 13 (1) (b).

<sup>88</sup> AMLD Art. 13 (1) (c).

<sup>89</sup> AMLD Art. 13 (1) (d).

<sup>90</sup> AMLD Arts. 18 to 24.

<sup>91</sup> AMLD Arts. 15 to 17.

<sup>92</sup> AMLD Art. 32 (1).

<sup>93</sup> AMLD Art. 32 (3).

<sup>94</sup> AMLD Art. 33 (1) (b).

<sup>95</sup> AMLD Art 32 (3).

judicial FIUs<sup>96</sup>. Most FIUs in the European Union are classified either as administrative (e.g. Belgium, France, Poland) or as police-type (e.g. Austria, Germany, Ireland)<sup>97</sup>.

The AMLD promotes cooperation among the FIUs of the Member States<sup>98</sup>. The FIUs should use protected communication channels, and the Directive specifically suggests the use of the FIU.net<sup>99</sup>. FIU.net is a decentralised computer system that facilitates data sharing among FIUs in the EU<sup>100</sup>. Since the system is decentralised, each FIU has complete control over its data and the persons who can access it. There are limitations as to how FIUs can use the information received from counterparts<sup>101</sup>. For instance, the transmitting FIU may impose conditions to the use of the information<sup>102</sup>. Additionally, if the receiving FIU wants to share the information with another authority from the receiving Member State, consent of the transmitting FIU is required prior to the transmission of the respective information<sup>103</sup>. Nonetheless, the different models of FIUs can complicate cooperation between the institutions<sup>104</sup>.

The subject of data protection for FIUs entails ample debate. The FIUs do not have a specific form according to EU law<sup>105</sup>. This difference complicates the application of data protection legislation to FIUs. Currently, there are FIUs that apply the General Data Protection Regulation (hereinafter GDPR)<sup>106</sup>, while others apply the Law Enforcement Directive<sup>107</sup> (hereinafter LED)<sup>108</sup>. This difference is problematic because the GDPR has a higher degree of protection of personal data than the LED<sup>109</sup>. This means

---

<sup>96</sup> Valsamis Mitsilegas, 'New Forms of Transnational Policing: The Emergence of Financial Intelligence Units in the European Union and the Challenges for Human Rights: Part 1', *Journal of Money Laundering Control* 3, no. 2 (1 January 1999): 147–60, <https://doi.org/10.1108/eb027226>.

<sup>97</sup> Mouzakiti, 'Cooperation between Financial Intelligence Units in the European Union', 354.

<sup>98</sup> AMLD Art. 52.

<sup>99</sup> AMLD Art. 56.

<sup>100</sup> Udo Kroon, 'Ma3tch: Privacy and Knowledge: "Dynamic Networked Collective Intelligence"', in *2013 IEEE International Conference on Big Data*, 2013, 24, <https://doi.org/10.1109/BigData.2013.6691683>.

<sup>101</sup> Mouzakiti, 'Cooperation between Financial Intelligence Units in the European Union', 359.

<sup>102</sup> AMLD Art. 54.

<sup>103</sup> AMLD Art. 55 (1).

<sup>104</sup> Mouzakiti, 'Cooperation between Financial Intelligence Units in the European Union', 354.

<sup>105</sup> Mitsilegas and Vavoula, 'The Evolving EU Anti-Money Laundering Regime', 282.

<sup>106</sup> 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance)', Pub. L. No. 32016R0679, 119 OJ L (2016), 67, <http://data.europa.eu/eli/reg/2016/679/oj/eng>.

<sup>107</sup> 'Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA', 119 OJ L § (2016), <http://data.europa.eu/eli/dir/2016/680/oj/eng>.

<sup>108</sup> Mouzakiti, 'Cooperation between Financial Intelligence Units in the European Union', 365.

<sup>109</sup> Ibid.

that, in the collaboration between FIUs, the personal data could go from a regime of more protection to a regime of less protection<sup>110</sup>.

### 3. THE ROLE OF PREVENTION IN ANTI-MONEY LAUNDERING

The classic model of money laundering involves three stages: placement, layering and integration. At the placement stage, money originating from illicit activities is placed in the financial system. That stage is of central importance for identifying suspicious activities of money laundering because the dirty money is still “close to its origin”<sup>111</sup>. Thus, money launderers are more vulnerable at this stage; that is, law enforcement agents can detect them more easily. Criminals do not always place their money in a financial institution. They may choose, instead, a cash-intensive type of business such as fast-food restaurants, parking garages or convenience stores to place the cash<sup>112</sup>. Subsequently, at the stage of layering, they perform successively several transactions with the money to obfuscate the origins of it<sup>113</sup>. The layering process distances the money from its origin and makes the money appear licit<sup>114</sup>. At the integration stage, money laundering is completed and the proceeds from criminal activity can be used for paying mainstream products and services without raising suspicions<sup>115</sup>.

There are two main models for anti-money laundering: the Swiss model and the American Model. The Swiss Model is based on *prevention*, while the American Model focuses on *repression*<sup>116</sup>. These models are not mutually exclusive. In fact, combining the methods can guarantee a more effective approach<sup>117</sup>. On the one side, the American Model aims at enforcing criminal measures that ultimately should lead to seizing proceeds originating from criminal activities<sup>118</sup>. On the other side, the Swiss Model proposes

---

<sup>110</sup> Ibid.

<sup>111</sup> Stessens, *Money Laundering*, 84; Levi and Reuter, ‘Money Laundering’, 311.

<sup>112</sup> Friedrich Schneider and Ursula Windischbauer, ‘Money Laundering: Some Facts’, *European Journal of Law and Economics* 26, no. 3 (1 December 2008): 395, <https://doi.org/10.1007/s10657-008-9070-x>; Stefan D. Cassella, ‘Toward a New Model of Money Laundering: Is the “Placement, Layering, Integration” Model Obsolete?’, *Journal of Money Laundering Control* 21, no. 4 (1 January 2018): 494, <https://doi.org/10.1108/JMLC-09-2017-0045>.

<sup>113</sup> Stessens, *Money Laundering*, 84.

<sup>114</sup> Cox, *Handbook of Anti-Money Laundering*, 17.

<sup>115</sup> Ibid., 18.

<sup>116</sup> Stessens, *Money Laundering*, 109.

<sup>117</sup> Ibid., 108.

<sup>118</sup> Ibid., 109.

mostly anti-money laundering rules, in order to protect the financial system of the country from being used/exploited by criminals<sup>119</sup>.

Repressive measures (traditionally) pertain to criminal law and may be directed to everyone within a legal order (considering the scope of the applicable law). On the contrary, preventive measures are usually directed at specific entities the social position of which makes them prone to being exploited for money laundering purposes – with financial institutions being the most representative example. Yet, while placing financial institutions at the centre of attention, money launderers switch their illicit activities to other entities<sup>120</sup>. Against this backdrop, the EU has expanded progressively the list of obliged institutions<sup>121</sup>, but the focus still lies on financial institutions.

The following analysis focuses on preventive measures to fight money laundering; that is, on measures conceived for financial institutions. However, it is important to reiterate that the preventive approach and the repressive approach may be intertwined. One model is not, nor should be considered, superior to the other. That said, the section below explains the challenges arising from KYC processes for money laundering prevention.

### **3.1. Challenges arising from the KYC requirements in the field of money laundering prevention**

The idea of having KYC processes at the service of the supervisor contrasts to the non-interference principle that banks traditionally have operated by<sup>122</sup>. Concerning the preventive approach to money laundering, it is expected that the identification requirements would dissuade money launders from trying to use the financial system to launder money<sup>123</sup>. Identification requirements could also be helpful for law enforcement agencies, that could request access to the identification of the parties involved in suspicious transactions.

---

<sup>119</sup> Ibid.

<sup>120</sup> Ibid., 135–36.

<sup>121</sup> Currently, the list of obliged natural and legal persons due to the professional activity has 10 items, including some definitions that are rather loose, such as “other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked”. 5th AMLD. Art. 2 (3) (e).

<sup>122</sup> Stessens, *Money Laundering*, 146.

<sup>123</sup> Ibid.

Appropriate KYC needs to analyse the information provided by the client in a critical way to assure that the information provided is reliable<sup>124</sup>. The issue of collecting inaccurate information should not be overlooked. The inaccurate information can arise from a mistake of the customer when filling forms and providing information<sup>125</sup>, but it may also be associated with malicious intentions of the customer<sup>126</sup>. Despite the importance of these processes, mandatory KYC can be costly for obliged entities. According to a survey conducted in Europe by LexisNexis with senior decision-makers for AML compliance, the costs of KYC Programmes sum up to approximately 40% of the total AML compliance costs – making them the highest cost among AML related ones<sup>127</sup>.

Even though anti-money laundering and KYC have been in practice for over 20 years now, financial institutions still see it as an obstacle to business growth. Research conducted in 42 countries in 2021 has shown that 72.4% of banks believe AML/KYC requirements are a barrier to servicing the global trade finance needs<sup>128</sup>. That was in fact the preeminent barrier to expanding business among the ones pointed in this research. KYC concerns seem to account for 10% of rejected applications for the trade finance<sup>129</sup>. This can be especially harmful to small and medium-sized enterprises (SMEs), since 40% of rejected applications refer to these companies, even though SMEs only account for 23% of the total number of applications<sup>130</sup>. This might be explained by the fact that larger companies, especially publicly listed ones, have a larger share of information that is publicly available<sup>131</sup>. Those companies are also subject to external audits and more scrutiny from the media<sup>132</sup>. This causes financial institutions to perceive that larger companies yield lower risks compared to SMEs<sup>133</sup>.

There are efforts to prevent this issue. Financial institutions have been using electronic channels to facilitate the process. Banks have been employing technology to

---

<sup>124</sup> Cox, *Handbook of Anti-Money Laundering*, 170.

<sup>125</sup> Ibid., 171.

<sup>126</sup> Ibid., 172.

<sup>127</sup> LexisNexis Risk Solutions, 'The True Cost of AML Compliance – European Survey European Edition', 9.

<sup>128</sup> Kijin Kim, Steven Beck, and Ma Concepcion Latoja, *2021 Trade Finance Gaps, Growth, and Jobs Survey* (Asian Development Bank, 2021), 3, <https://www.adb.org/publications/2021-trade-finance-gaps-growth-jobs-survey>.

<sup>129</sup> Ibid., 5.

<sup>130</sup> Ibid.

<sup>131</sup> Cox, *Handbook of Anti-Money Laundering*, 199.

<sup>132</sup> Ibid.

<sup>133</sup> Ibid.

facilitate compliance checks<sup>134</sup>. As physical exchanges have been avoided ever since the COVID-19 pandemic, this might push the use of digital channels and the technologies used might contribute to making access to financial institutions more equalized. Nonetheless, the use of digital channels also involves risks. In the Internet Organised Crime Threat Assessment (hereinafter IOCTA) 2021 Report, Europol warns that criminals might take advantage of the use of electronic channels and of the pandemic to commit online fraud<sup>135</sup>. For instance, criminals may call citizens claiming that they need their identification to schedule vaccination<sup>136</sup>. In countries where mobile bank ID is linked to medical services, this can allow criminals to access citizens bank accounts and transfer money from these accounts<sup>137</sup>.

Apart from small businesses, strict identification requirements might also lead to exclusion of specific groups presenting particularities that keep them from having regular means of identification, such as a passport or a driver license<sup>138</sup>. For instance, according to estimations of the World Bank Group, there was a billion people without official proof of identity worldwide in 2018<sup>139</sup>. Another of the identification aspects required by KYC processes that could limit access refers to proof-of-residence, which might leave out people with no stable living situations. Boat-dwellers and refugees are examples of people that could be excluded from the financial system due to strict KYC requirements<sup>140</sup>. KYC aspects might also be burdensome for people in vulnerable situations and living in rural communities<sup>141</sup>.

KYC also entails privacy concerns. Data protection is an increasing concern for Europeans. A survey conducted by the European Union Agency for Fundamental Rights has shown that 55% of the respondents are concerned about criminals or fraudsters accessing personal information they share on the Internet without their knowledge.<sup>142</sup> KYC principle necessarily implies some loss of the clients' privacy. For instance, by having to abide by customers' identification, financial institutions can no longer allow

---

<sup>134</sup> Kim, Beck, and Latoja, *2021 Trade Finance Gaps, Growth, and Jobs Survey*, 6.

<sup>135</sup> Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2021* (Luxembourg: Publications Office of the European Union, 2021), 32.

<sup>136</sup> Ibid.

<sup>137</sup> Ibid.

<sup>138</sup> Gill and Taylor, 'Preventing Money Laundering or Obstructing Business?', 588.

<sup>139</sup> World Bank Group, 'Data Visualization | Identification for Development', ID4D, accessed 6 December 2021, <https://id4d.worldbank.org/global-dataset/visualization>.

<sup>140</sup> Gill and Taylor, 'Preventing Money Laundering or Obstructing Business?', 588.

<sup>141</sup> Arner et al., 'The Identity Challenge in Finance', 57.

<sup>142</sup> European Union Agency for Fundamental Rights., *Your Rights Matter: Data Protection and Privacy: Fundamental Rights Survey*. (LU: Publications Office, 2020), <https://data.europa.eu/doi/10.2811/292617>.

customers to maintain anonymous accounts. Those interested in protecting their privacy from the financial system may not have many options left.

Since the obliged entities are controlling personal data, they should also comply with the GDPR. At EU level, processing of personal data for money-laundering prevention is considered a matter of public interest<sup>143</sup>. According to the GDPR, data processing for the performance of a task carried out in the public interest is lawful<sup>144</sup>.

To protect the rights of the data subjects, the obliged entities must implement data protection by design and by default<sup>145</sup>. This includes employing technical and organisational features that should ensure that the data is not accessible to an indefinite number of natural persons<sup>146</sup>. All these requirements can add sizable costs to obliged entities. A survey conducted by IAPP-EY in 2021 found that the average amount an organisation spent on privacy in 2021 was 873,000 dollars<sup>147</sup>.

Although the costs of compliance are high, failing to comply with data protection regulations can yield even higher costs. According to a 2021 study conducted by IBM Corporation, the average total cost of a data breach in the financial sector is 5.72 million dollars<sup>148</sup>. This report also indicated that the most common data breach refers to customers' personal information. The costs considered for this study include detecting the event, notification of the data subjects affected by the breach, business loss, and post-breach response<sup>149</sup>. The numbers presented above can indicate that obliged entities need to apply a lot of resources in data protection.

### **3.2. Clusters of challenges arising from KYC requirements**

Succinctly, the challenges arising from KYC can be divided into three areas: costs for complying with KYC requirements, exclusion of clients and complex data protection. It was shown above that KYC requirements represent an important part of the business costs of financial institutions and obliged entities. Individuals can be excluded from the financial system, as strict KYC requirements can be prohibitive to people without identification and stable residency. The source of funds requirements can affect certain

---

<sup>143</sup> AMLD Art. 43.

<sup>144</sup> GDPR Art. 6 (1) (e).

<sup>145</sup> GDPR Art. 25.

<sup>146</sup> GDPR Art. 25 (2).

<sup>147</sup> IAPP-EY, 'IAPP-EY Annual Privacy Governance Report 2021', 2021, 36, [https://iapp.org/media/pdf/resource\\_center/IAPP\\_EY\\_Annual\\_Privacy\\_Governance\\_Report\\_2021.pdf](https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf).

<sup>148</sup> IBM Corporation, 'Cost of a Data Breach Report 2021', July 2021, 15.

<sup>149</sup> Ibid., 9.



types of companies, such as SMEs. The last challenge is protecting the data collected with KYC according to data protection regulations. This affects individuals, because they need to present their personal data to financial institutions if they want to establish a business relationship with them. Moreover, financial institutions and obliged entities that are collecting personal data in the course of their business relationship need to comply with rigid data protection requirements laid out by the GDPR.

The table below shows the clusters of challenges arising from KYC requirements:

<b>Challenges Arising From KYC Requirements</b>	<b>Affected Entities</b>		
KYC Compliance Costs	Financial Institutions and Obligated Entities		
Financial Exclusion	SMEs	Individuals Without identification	Individuals Without Stable Residency
Data Protection Implications	Financial Institutions and Obligated Entities	Individuals	

#### **4. CONTROVERSIES ASSOCIATED WITH THE USE OF CRYPTOCURRENCIES**

Generally, cryptocurrencies are associated with price volatility<sup>150</sup> and crime<sup>151</sup>. According to CipherTrace, a company specialized in cryptocurrency intelligence and

<sup>150</sup> In the course of only three weeks, there is news indicating an all-time record, followed by a crash of 20%. Julia Kollwe, 'Bitcoin Price Surges to Record High of More than \$68,000', *The Guardian*, 9 November 2021, sec. Technology, <https://www.theguardian.com/technology/2021/nov/09/bitcoin-price-record-high-cryptocurrencies-ethereum>; 'Bitcoin Retreats 20% From Record, Joining Risk-Asset Sell-Off', *Bloomberg.Com*, 26 November 2021, <https://www.bloomberg.com/news/articles/2021-11-26/bitcoin-retreats-20-from-all-time-high-set-earlier-in-november>.

<sup>151</sup> E.g. Tom Wilson, 'Crime at Crypto "DeFi" Sites Hits \$10.5 Bln in 2021, Research Shows', *Reuters*, 19 November 2021, sec. Technology, <https://www.reuters.com/technology/crime-crypto-defi-sites-hits-105-bln-2021-research-shows-2021-11-18/>; "'Bitcoin Fraud Cost Me £500,000'", *BBC News*, 4 September 2021, sec. Business, <https://www.bbc.com/news/business-58424832>; Helen Pidd, 'Man Jailed for Kidnapping Boy Who Was Said to Have Made Money from Bitcoin', *The Guardian*, 18 October 2021, sec.

forensics, cryptocurrency-related thefts, hacks, and frauds totalized \$681 million only in the first semester of 2021<sup>152</sup>. Europol states that, although there are different estimates about the share of illicit activities happening on cryptocurrencies, as the absolute number of cryptocurrency transactions grow, the absolute amount of illicit activities grows as well<sup>153</sup>.

Corbet *et al.* divide cryptocurrency cyber criminality into two forms: cyber criminality originated in the use of cryptocurrencies and cyber criminality directly attacking structures of cryptocurrency<sup>154</sup>. In the first case, the use of cryptocurrencies may enable payment for illegal goods, such as narcotics. This was the case of Silk Road, a marketplace based in the Dark Web, whose products ranged from mainstream goods, such as clothing items, to illegal ones, such as illegal drugs<sup>155</sup>. The transactions in Silk Road could be settled using Bitcoin<sup>156</sup>. On the other hand, there are also cases in which cyber criminals attack the structures of cryptocurrencies<sup>157</sup>. Initial coin offerings<sup>158</sup> (hereinafter ICOs) are mechanisms that are often attacked by hackers. It is estimated that more than 10% of funds raised ICOs are stolen by hackers<sup>159</sup>. ICOs are able to raise large sums of money<sup>160</sup>, which can be exploited by fraudsters. For instance, in 2017, a Belize-based company named Dropil inc. launched an ICO that promised access to an automated trading bot<sup>161</sup>. The company lied to investors about the profitability of the trading bot and

---

UK news, <https://www.theguardian.com/uk-news/2021/oct/18/man-jailed-for-kidnapping-boy-who-was-said-to-have-made-money-from-bitcoin>.

<sup>152</sup> CipherTrace, ‘Cryptocurrency Crime and Anti-Money Laundering Report (2021)’ (CipherTrace, August 2021), 6, <https://info.ciphertrace.com/hubfs/CAML%20Reports/Cryptocurrency%20Crime%20and%20Anti-Money%20Laundering%20Report%2c%20August%202021.pdf>.

<sup>153</sup> Europol, *Cryptocurrencies: Tracing the Evolution of Criminal Finances*. (LU: Publications Office, 2021), 5, <https://data.europa.eu/doi/10.2813/75468>.

<sup>154</sup> Shaen Corbet et al., ‘Cryptocurrencies as a Financial Asset: A Systematic Analysis’, *International Review of Financial Analysis* 62 (1 March 2019): 13, <https://doi.org/10.1016/j.irfa.2018.09.003>.

<sup>155</sup> Ibid.; Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction*, Second edition (London ; New York: Routledge, Taylor & Francis Group, 2018), 22.

<sup>156</sup> Holt, Bossler, and Seigfried-Spellar, *Cybercrime and Digital Forensics*, 22; Corbet et al., ‘Cryptocurrencies as a Financial Asset’, 13.

<sup>157</sup> Corbet et al., ‘Cryptocurrencies as a Financial Asset’, 13.

<sup>158</sup> According to an OECD report, “Initial Coin Offerings (ICOs) consist of the creation of digital tokens by start-up companies (i.e. young micro-SMEs) and their distribution to investors in exchange for fiat currency or, in most cases, mainstream cryptocurrencies”. OECD, ‘Initial Coin Offerings (ICOs) for SME Financing’, 2019, 9, [www.oecd.org/finance/initial-coin-offerings-for-sme-financing.htm](http://www.oecd.org/finance/initial-coin-offerings-for-sme-financing.htm).

<sup>159</sup> Ernst & Young, ‘EY Research: Initial Coin Offerings (ICOs)’, 2018, 31, [https://assets.ey.com/content/dam/ey-sites/ey-com/en\\_gl/topics/banking-and-capital-markets/ey-research-initial-coin-offerings-icos.pdf](https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-research-initial-coin-offerings-icos.pdf); Corbet et al., ‘Cryptocurrencies as a Financial Asset’, 13.

<sup>160</sup> Paul P. Momtaz, ‘Initial Coin Offerings’, *PLOS ONE* 15, no. 5 (21 May 2020): 7, <https://doi.org/10.1371/journal.pone.0233018>.

<sup>161</sup> ‘Two O.C. Men Agree to Plead Guilty to Securities Fraud Charge for Swindling Investors Through \$1.8 Million Cryptocurrency Offering’, United States Department of Justice, 2 July 2021,

of the ICO itself<sup>162</sup>. Yet, it was able to raise 1.8 million dollars<sup>163</sup>. ICOs can also be used by criminals to launder money. To illustrate this case, a money launderer can purchase newly issued tokens in an ICO<sup>164</sup>. In this case, turning the funds into new tokens can distance the money from its origins. After the ICO, the tokens can be traded into other cryptocurrencies and even into fiat money<sup>165</sup>.

The hacks can also be performed against cryptocurrency wallets and against cryptocurrency service providers<sup>166</sup>. As an example, in 2016, 120,000 bitcoins were stolen from the cryptocurrency exchange service provider Bitfinex<sup>167</sup>. In this case, the bitcoins were stolen from the users' wallets and sent to a single wallet<sup>168</sup>.

Ransomware attacks are also often associated with the use of cryptocurrencies – with criminals demanding ransom to be paid in Bitcoin or other cryptocurrencies<sup>169</sup>. Ransomware is a type of software that blocks access to a computer system or file (keeping it 'hostage') and demands the payment of ransom to give back access<sup>170</sup>. The IOCTA 2021 Report indicates that criminals have been focusing their efforts on large private companies and governmental institutions, as those targets are more likely to have the financial means required to pay the ransom and they usually need to re-establish their function urgently<sup>171</sup>. For instance, in May 2021, cybercriminals attacked the Irish health system (HSE) causing a reduction in the number of outpatient appointments<sup>172</sup>. In this case, the criminals requested twenty million dollars to give the encryption key that would allow access to the system<sup>173</sup>. A week after the attack, the criminals provided that key for

---

<https://www.justice.gov/usao-cdca/pr/two-oc-men-agree-plead-guilty-securities-fraud-charge-swindling-investors-through-18>.

<sup>162</sup> Ibid.

<sup>163</sup> Ibid.

<sup>164</sup> OECD, 'Initial Coin Offerings (ICOs) for SME Financing', 36.

<sup>165</sup> Ibid.

<sup>166</sup> Corbet et al., 'Cryptocurrencies as a Financial Asset', 14.

<sup>167</sup> 'Bitcoin Worth \$72 Million Stolen from Bitfinex Exchange in Hong Kong', *Reuters*, 3 August 2016, sec. Banks, <https://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP>.

<sup>168</sup> Ibid.

<sup>169</sup> Europol, *Cryptocurrencies*, 17.

<sup>170</sup> Bart Custers, Jan-Jaap Oerlemans, and Ronald Pool, 'Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies', *European Journal of Crime, Criminal Law and Criminal Justice* 28, no. 2 (9 July 2020): 122, <https://doi.org/10.1163/15718174-02802002>.

<sup>171</sup> Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2021*, 20.

<sup>172</sup> Michael Sheils McNamee, 'HSE Cyber-Attack: Irish Health Service Still Recovering Months after Hack', *BBC News*, 5 September 2021, sec. Europe, <https://www.bbc.com/news/world-europe-58413448>.

<sup>173</sup> Ibid.

free<sup>174</sup>. However, the cybercriminals still demanded the payment of ransom, threatening to publish data stolen in this attack if the payment was not done<sup>175</sup>.

Furthermore, criminals often target users that are interested in cryptocurrencies as an investment. Since earlier adopters of cryptocurrencies saw tremendous increase in the price of bitcoin, the users of cryptocurrencies can be more prone to believing in fraudsters promising high returns<sup>176</sup>. The criminals promise high returns and present Bitcoin as an investment opportunity<sup>177</sup>. These investment scams are often Ponzi schemes<sup>178</sup>. One example is the BitConnect case, a Ponzi scheme that operated worldwide from 2017 to 2018<sup>179</sup>. The scheme promised investors high earnings from exchanges on cryptocurrency markets. It is estimated that two billion dollars were stolen from the victims.

It is necessary to explore technical aspects of cryptocurrency to assess whether the technical aspects are related to the criminal activity taking place in association with cryptocurrencies. The following analysis focuses on the anonymity inherent in the design of cryptocurrencies and on how criminals have noticed this so quickly (that is, before it became a matter of public discourse). Before that, it is necessary to further explore what cryptocurrencies are, and, particularly, which is the technology behind them.

Thus, Section 4.1 explains briefly some of the technical aspects of cryptocurrencies and delineates the historical background of their development. Section 4.2 delves into anonymity in terms of a key element of cryptocurrencies. Finally, Section 4.3 discusses why criminals find cryptocurrencies attractive.

---

<sup>174</sup> Joe Tidy, 'Irish Cyber-Attack: Hackers Bail out Irish Health Service for Free', *BBC News*, 21 May 2021, sec. Europe, <https://www.bbc.com/news/world-europe-57197688>.

<sup>175</sup> Ibid.

<sup>176</sup> Securities and Exchange Commission, 'Investor Alert: Bitcoin and Other Virtual Currency-Related Investments', 2014, [https://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia\\_bitcoin.html](https://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html).

<sup>177</sup> Ibid.

<sup>178</sup> "A Ponzi scheme is an investment scam that involves the payment of purported returns to existing investors from funds contributed by new investors. Ponzi scheme organizers often solicit new investors by promising to invest funds in opportunities claimed to generate high returns with little or no risk. In many Ponzi schemes, rather than engaging in any legitimate investment activity, the fraudulent actors focus on attracting new money to make promised payments to earlier investors as well as to divert some of these "invested" funds for personal use." Securities and Exchange Commission, 'Ponzi Schemes Using Virtual Currencies', 2013, 1, [https://www.sec.gov/investor/alerts/ia\\_virtualcurrencies.pdf](https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf).

<sup>179</sup> Securities and Exchange Commission, 'SEC Charges Global Crypto Lending Platform and Top Executives in \$2 Billion Fraud', 2021, <https://www.sec.gov/news/press-release/2021-172>.

#### 4.1. Understanding Blockchain and the origins of Cryptocurrencies

According to Corbet, “[c]ryptocurrencies are peer-to-peer electronic cash systems which allow online payments to be sent directly from one party to another without going through a financial institution”<sup>180</sup>.

The idea of a digital cash system was first proposed by David Chaum in 1983. His idea was that the cryptography he introduced (blind signature) would permit “realization of untraceable payments systems which offer improved auditability and control compared to current systems, while at the same time offering increased personal privacy”<sup>181</sup>. Compared to Chaum’s ideas, the main innovation introduced by Bitcoin (the first cryptocurrency) was the possibility of storing this information in a blockchain structure rather than in a server run by a central authority<sup>182</sup>.

Although blockchain has been at the centre of public attention for many years now, there is little understanding of how it works<sup>183</sup>. A 2017 Study from HSBC on Trust in Technology has shown that 80% of the 12,019 participants could not understand Blockchain and 59% of them had never heard about it<sup>184</sup>.

Blockchain, in a nutshell, is a database in which any new piece of data added is stored in a so-called block<sup>185</sup>. Blocks are organised in such a way that every new block is dependent on the previous one<sup>186</sup>. This database is not stored in a single central server. Instead, it is stored in all the computers of the users – which are called nodes – of the network in a distributed ledger technology (DLT) design<sup>187</sup>. A newly added block needs to be approved by the nodes, which happens through a consensus algorithm<sup>188</sup>.

If a blockchain is public, it will not require a central authority. In public blockchains (permissionless), there are no requirements for someone to join and act in the

---

<sup>180</sup> Corbet et al., ‘Cryptocurrencies as a Financial Asset’, 3.

<sup>181</sup> David Chaum, ‘Blind Signatures for Untraceable Payments’, in *Advances in Cryptology*, ed. David Chaum, Ronald L. Rivest, and Alan T. Sherman (Boston, MA: Springer US, 1983), 203, [https://doi.org/10.1007/978-1-4757-0602-4\\_18](https://doi.org/10.1007/978-1-4757-0602-4_18).

<sup>182</sup> Arvind Narayanan, ‘Foreword: The Long Road to Bitcoin’, in *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton: Princeton University Press, 2016).

<sup>183</sup> Garrick Hileman and Michel Rauchs, ‘2017 Global Blockchain Benchmarking Study’, *SSRN Electronic Journal*, 2017, 13, <https://doi.org/10.2139/ssrn.3040224>.

<sup>184</sup> ‘Trust in Technology’ (HSBC, 2017), 12.

<sup>185</sup> Arvind Narayanan, ‘Introduction to Cryptography and Cryptocurrencies’, in *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton: Princeton University Press, 2016).

<sup>186</sup> Ibid.

<sup>187</sup> Arvind Narayanan, ‘How Bitcoin Achieves Decentralization’, in *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton: Princeton University Press, 2016).

<sup>188</sup> Ibid.

blockchain<sup>189</sup>. In this system, the integrity of the data is established by cryptography, which is enabled by having the information repeatedly stored in several different nodes<sup>190</sup>. The system is called trustless because one does not have to trust a third party to guarantee data integrity. Nevertheless, a blockchain can be private and centralised. In such a case, there will be a list of allowed users and their permissions<sup>191</sup>.

Cryptocurrencies are based on blockchain technology, but the technology itself enables a lot more than the transaction of monetary assets. Blockchain may be used for storing any kind of data. The DLT was explored for the first time in 1991 when the article "How to Time Digital Stamp Documents" was published by W. Scott Stornetta and Stuart Haber. Aiming to address the growing incidence of videos, images and audios that can be modified easily through computers, the authors propose a method of timestamping documents through Blockchain to guarantee the authenticity of files. Blockchain is applied in multiple areas, including education (e.g., authenticating diplomas<sup>192</sup>), public governance (e.g., notary<sup>193</sup>, identity management<sup>194</sup>, etc.), and health (e.g., electronic healthcare records<sup>195</sup>)<sup>196</sup>.

Cryptocurrencies are probably the most well-known application of blockchain. In this case, the blocks store the data of transactions performed online.

Satoshi Nakamoto (the pseudonym for the yet unknown creator/creators of bitcoin) proposed the creation of a "peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power"<sup>197</sup>. In online transactions, merchants and customers need to trust third parties for the processing of

---

<sup>189</sup> Fran Casino, Thomas K. Dasaklis, and Constantinos Patsakis, 'A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues', *Telematics and Informatics* 36 (1 March 2019): 57, <https://doi.org/10.1016/j.tele.2018.11.006>.

<sup>190</sup> Natarajan, Krause, and Gradstein, 'Distributed Ledger Technology and Blockchain', 2017, X,6.

<sup>191</sup> Casino, Dasaklis, and Patsakis, 'A Systematic Literature Review of Blockchain-Based Applications', 57.

<sup>192</sup> Blockcerts, 'Blockchain Credentials', Blockcerts, accessed 29 March 2021, <http://blockcerts.org/>.

<sup>193</sup> Rohan Pinto, 'Council Post: A Blockchain-Based Digital Notary: What You Need To Know', Forbes, 2019, <https://www.forbes.com/sites/forbestechcouncil/2019/11/12/a-blockchain-based-digital-notary-what-you-need-to-know/>.

<sup>194</sup> 'Blockchain for Digital Identity - IBM Blockchain | IBM', accessed 29 March 2021, <https://www.ibm.com/blockchain/solutions/identity>.

<sup>195</sup> Asaph Azaria et al., 'MedRec: Using Blockchain for Medical Data Access and Permission Management', in *2016 2nd International Conference on Open and Big Data (OBD)* (2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria: IEEE, 2016), 25–30, <https://doi.org/10.1109/OBD.2016.11>.

<sup>196</sup> Casino, Dasaklis, and Patsakis, 'A Systematic Literature Review of Blockchain-Based Applications', 62–65.

<sup>197</sup> Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', 2008, 8.

payments and mediating disputes. These dispute mediation systems might allow for frauds performed by the consumers, which compels merchants to demand data that would otherwise be unnecessary in face-to-face transactions<sup>198</sup>. Instead of a third-party service provider, Bitcoin proposes a payment system without a trusted party<sup>199</sup>. In Bitcoin, there are specialised nodes responsible for creating and keeping track of the created blocks<sup>200</sup>. These nodes are called miners<sup>201</sup>. Once a block is created and accepted by other miners, the transaction is irreversible. According to Nakamoto, having irreversible transactions combined with routine escrow mechanisms would protect sellers and buyers respectively<sup>202</sup>. However, the “routine escrow mechanisms” have never been implemented on Bitcoin<sup>203</sup>.

In practice, cryptocurrency users often utilize services from a cryptocurrency exchange to buy and sell bitcoins and other cryptocurrencies. Cryptocurrency exchanges match supply and demand, contributing to price discovery<sup>204</sup>. The services of cryptocurrency serve to send cryptocurrency to other users, but also to exchange cryptocurrency for fiat currencies or vice-versa<sup>205</sup>. From the user point of view, cryptocurrency exchanges can resemble banks since you can keep your cryptocurrencies in the exchange and send them to other users through its interface<sup>206</sup>. Cryptocurrency exchanges can be either centralised or decentralised. Centralised exchanges are the most popular kind of cryptocurrency exchange. Centralised exchanges are characterized by a central structure that ultimately operates the trades<sup>207</sup>. They are also called custodian exchanges because they can keep custody of their client’s assets. Decentralised exchanges (hereinafter DEXs), on the other hand, are offered by platforms that operate smart contract protocols (often based on the Ethereum blockchain), which are responsible for matching demand with supply<sup>208</sup>.

---

<sup>198</sup> Ibid., 1.

<sup>199</sup> Ibid.

<sup>200</sup> Narayanan, ‘Foreword: The Long Road to Bitcoin’.

<sup>201</sup> Ibid.

<sup>202</sup> Nakamoto, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’, 1.

<sup>203</sup> Pietro Ortolani, ‘The Impact of Blockchain Technologies and Smart Contracts on Dispute Resolution: Arbitration and Court Litigation at the Crossroads’, *Uniform Law Review*, 16 May 2019, 433–34, <https://doi.org/10.1093/ulr/unz017>.

<sup>204</sup> Garrick Hileman and Michel Rauchs, ‘2017 Global Cryptocurrency Benchmarking Study’, *SSRN Electronic Journal*, 2017, 28, <https://doi.org/10.2139/ssrn.2965436>.

<sup>205</sup> Arvind Narayanan, ‘How to Store and Use Bitcoins’, in *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton: Princeton University Press, 2016).

<sup>206</sup> Ibid.

<sup>207</sup> van Duyne, Harvey, and Gelemerova, *The Critical Handbook of Money Laundering*, 128.

<sup>208</sup> Will Warren and Amir Bandeali, ‘0x: An Open Protocol for Decentralized Exchange on the Ethereum Blockchain’ (2017).

The aim behind the development of Bitcoin was to make online payments easier and less costly<sup>209</sup>. However, so far, it does not seem like the infrastructure of cryptocurrencies replaces financial institutions, but it is rather a complement to the standard banking markets<sup>210</sup>. One of the reasons why it is hard for Bitcoin to gain traction is the price volatility<sup>211</sup>. Performing a sale using Bitcoin or any other cryptocurrency as a means of payment would mean severe volatility in the price of the product. This volatility makes it harder for merchants to price their products, and, thus, they are not willing to accept Bitcoins or other cryptocurrencies. Furthermore, owning and using cryptocurrencies requires a level of technical knowledge higher than the know-how required to perform online payments traditionally by means, for instance, of credit cards.

Moreover, as Bitcoin grew in fame, its proof-of-work system has proved costly energy-wise.<sup>212</sup> Through this model, the nodes should compete to solve complex computational problems for verifying each transaction. This model spends a significant amount of energy, and with the growth of the network, it becomes extremely costly for small miners<sup>213</sup>. Although it is very hard to have exact numbers, as miners are often anonymous, some authors argue that the energy consumption of bitcoin could be comparable to the energy consumption of a country such as Ireland<sup>214</sup>.

## **4.2. Anonymity: a key factor of the use of cryptocurrencies**

The development of new technologies can assist regulators, compliance officers and law enforcement agencies in Money Laundering Prevention. The use of technology as an aid for regulatory monitoring, reporting and compliance is called RegTech<sup>215</sup>.

---

<sup>209</sup> Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', 1.

<sup>210</sup> Ed Saiedi, Anders Broström, and Felipe Ruiz, 'Global Drivers of Cryptocurrency Infrastructure Adoption', *Small Business Economics* 57, no. 1 (1 June 2021): 384, <https://doi.org/10.1007/s11187-019-00309-8>.

<sup>211</sup> David Yermack, 'Is Bitcoin a Real Currency? An Economic Appraisal', Working Paper, Working Paper Series (National Bureau of Economic Research, December 2013), <https://doi.org/10.3386/w19747>.

<sup>212</sup> Alex de Vries, 'Bitcoin's Growing Energy Problem', *Joule* 2, no. 5 (16 May 2018): 804, <https://doi.org/10.1016/j.joule.2018.04.016>.

<sup>213</sup> There are cryptocurrencies that explore other models. For instance, another possible model is the proof-of-stake. In this model, there is no competition, and each validator has to leave an amount of its cryptocurrency at stake, which can be lost if the validator fails to do its job or does so in a malicious way (Ethereum staking, [s.d.]).

<sup>214</sup> K. J. O'Dwyer and D. Malone, 'Bitcoin Mining and Its Energy Footprint', 1 January 2014, 283, <https://doi.org/10.1049/cp.2014.0699>.

<sup>215</sup> Douglas W. Arner, Janos Nathan Barberis, and Ross P. Buckley, 'FinTech, RegTech and the Reconceptualization of Financial Regulation', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 1 October 2016), 4, <https://papers.ssrn.com/abstract=2847806>.



RegTech can enable automated monitoring of financial information and the use of artificial intelligence can even provide insides on issues and potential breaches before illegal activities take place<sup>216</sup>. Just as technology can support AML efforts, technological advancements/developments can be exploited by criminals.

The online world permits greater privacy when compared to the offline one<sup>217</sup>. According to *Lusthaus*, criminals in an offline world already have a known identity that needs to be concealed to increase their anonymity<sup>218</sup>. Inversely, cybercriminals have no identity by default and can partially reduce their anonymity to acquire online criminal partners<sup>219</sup>. Overall, the online environment offers more means for hiding identities than the offline environment. Merchants involved in online transactions remediate the anonymity issue since the transactions are completed through service providers that perform proper CDD of the parties and arbitrate disputes which may arise in online transactions. Cryptocurrencies propose a peer-to-peer model in which, ideally, there are no intermediaries<sup>220</sup>. Hence, the level of privacy that is already allowed by the Internet increases in transactions performed by means of cryptocurrencies.

According to *Lansky* cryptocurrency accounts can be divided into four groups depending on the level of privacy: transparent account, semi-transparent account, pseudo-anonymous account, anonymous account<sup>221</sup>. In a transparent account, the user discloses publicly his/her identity in a credible way<sup>222</sup>. In a semi-transparent account, at least one state administration can trace the owner of that account<sup>223</sup>. This is the case, for instance, when a customer uses a crypto-currency service provider that maintains KYC policies<sup>224</sup>. In a pseudo-anonymous account, other than the owner, the business counterparties are the only parties with information that can identify the owner of the account (e.g. IP address, face)<sup>225</sup>. Finally, in anonymous accounts, only the owner knows about the ownership of the account<sup>226</sup>. Anonymous accounts are only possible if the account is new or if the

---

<sup>216</sup> *Ibid.*, 14–15.

<sup>217</sup> Holt, Bossler, and Seigfried-Spellar, *Cybercrime and Digital Forensics*, 21.

<sup>218</sup> Jonathan Lusthaus, 'Trust in the World of Cybercrime', *Global Crime* 13, no. 2 (1 May 2012): 80, <https://doi.org/10.1080/17440572.2012.674183>.

<sup>219</sup> *Ibid.*

<sup>220</sup> Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', 3.

<sup>221</sup> Jan Lansky, 'Possible State Approaches to Cryptocurrencies', *Journal of Systems Integration* 9, no. 1 (31 January 2018): 22, <https://doi.org/10.20470/jsi.v9i1.335>.

<sup>222</sup> *Ibid.*

<sup>223</sup> *Ibid.*

<sup>224</sup> *Ibid.*

<sup>225</sup> *Ibid.*

<sup>226</sup> *Ibid.*

counterparties transacting with that account have lost or forgotten information that could identify the focal entity<sup>227</sup>. According to this classification, most accounts are pseudo-anonymous accounts. However, since many jurisdictions impose for virtual asset service providers (hereinafter VASPs) to have proper KYC of their clients, semi-transparent accounts might be/become more common.

Although the privacy provided by cryptocurrencies is often referred to as anonymity, most cryptocurrencies only allow for pseudo-anonymity<sup>228</sup>. It is called pseudo-anonymity because the users are in fact identified by other means, namely, through a pseudonym. There is no extensive CDD, the users do not have a formal identification (for instance, passport, ID, social security number), but the transacting parties are identified by their cryptocurrency account addresses<sup>229</sup>. That said, although it is not possible to easily access the information from the users behind those addresses, there is some sort of identification. As users make more and more transactions using the same account, the level of privacy decreases. For instance, by transacting with someone using cryptocurrency as means of payment, I reveal my account to the person I am transacting with<sup>230</sup>; i.e., this person is now able to link that account to me. In other words: every time one performs such a transaction, (s)he gives up some of his/her anonymity.

Additionally, in most cryptocurrencies the transactions are not hidden, they are in fact public; anyone can access all transactions and know right away that Account A has sent an X amount of Cryptocurrency to Account B. Cryptocurrencies may only allow for pseudo-anonymity, but this already complicates the work of law enforcement agencies. Going through a record with millions of transactions identified merely by pseudonyms to identify the malicious ones requires proper data analysis tools and qualified personnel. The IOCTA 2021 Report has highlighted the necessity of officers, tools and training for addressing cyber criminality<sup>231</sup>. According to the report, creating data analysis tools for tracing and decrypting cryptocurrencies are crucial for investigating cybercrime<sup>232</sup>. The report also highlights the success of operation DisrupTor, a collaborative operation involving German Federal Criminal Police (Bundeskriminalamt), the Dutch National

---

<sup>227</sup> Ibid.

<sup>228</sup> Steven David Brown, 'Cryptocurrency and Criminality: The Bitcoin Opportunity', *The Police Journal: Theory, Practice and Principles* 89, no. 4 (December 2016): 5, <https://doi.org/10.1177/0032258X16658927>.

<sup>229</sup> Lansky, 'Possible State Approaches to Cryptocurrencies', 21.

<sup>230</sup> Ibid., 22.

<sup>231</sup> Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2021*, 39.

<sup>232</sup> Ibid.

Police (Politie), Europol, Eurojust and US government agencies, which identified and arrested 179 vendors that operated in a Dark Web marketplace<sup>233</sup>. The operation relied on data from the takedown of the Wall Street Marketplace in May 2019, to overcome encryption and anonymity of cybercriminals<sup>234</sup>.

Pseudo-anonymity and the irreversibility of transactions may be problematic from a regulatory and law enforcement point of view. However, those characteristics of Bitcoin and other cryptocurrencies are precisely what attract most of their users. That does not refer only to criminals, but there are also groups of people that feel bothered by the oversight of government and wish to be under the radar for ideological reasons.

There were cryptocurrency projects attempting to solve the anonymity issue, but those projects were not successful. For instance, in 2018, a non-profit organisation launched a project to create a cryptocurrency network named ‘Sögur’ (previously named ‘Saga’), which would require users of the network to undergo KYC and AML procedures<sup>235</sup>. According to the organization, its advisory council included a JPMorgan Chase International chairman and a Nobel Laureate in Economic Sciences<sup>236</sup>. Nonetheless, in January 2021, a note was published on the website of the project announcing the end of it<sup>237</sup>. Earlier, in 2014, a group of developers created a “non-anonymous” cryptocurrency named Global Denomination<sup>238</sup>. The idea behind the coin was that users who are not interested in operating in dark markets or illegal activities would find value in a coin that offered no anonymity<sup>239</sup>. Nonetheless, this cryptocurrency seems to have failed, as the website is no longer available. One of the last posts the developers of this coin made in online forums was in November 2014<sup>240</sup>. There, they stated that the cryptocurrency was having troubles due to the lack of “community involvement”<sup>241</sup>.

---

<sup>233</sup> Ibid., 38.

<sup>234</sup> Ibid.

<sup>235</sup> ‘Sögur’s Whitepaper’, Sögur, accessed 31 January 2022, <https://www.sogur.com/whitepaper/>; Annaliese Milano, ‘A Non-Anonymous Stablecoin? Saga Launches With Big-Shot Advisor Team’, 22 March 2018, <https://www.coindesk.com/markets/2018/03/22/a-non-anonymous-stablecoin-saga-launches-with-big-shot-advisor-team/>.

<sup>236</sup> ‘Sögur Currency (SGR): Overview | LinkedIn’, accessed 1 February 2022, <https://www.linkedin.com/company/sogurcurrency/>.

<sup>237</sup> ‘Sögur’, accessed 31 January 2022, <https://www.sogur.com/>.

<sup>238</sup> ‘Global Denomination: Coin Dev Interview | Bitcoinist.Com’, 25 July 2014, <https://bitcoinist.com/global-denomination-coin-dev-interview/>.

<sup>239</sup> Ibid.

<sup>240</sup> ‘Global Denomination (GDN) X11 DigiShield’, accessed 31 January 2022, <https://bitcointalk.org/index.php?topic=578574.1460>.

<sup>241</sup> Ibid.

On the contrary, there are new coins that attempt to provide increased anonymity. Cryptocurrencies, such as Z-Cash<sup>242</sup> and Monero<sup>243</sup>, use different cryptographic protocols that increase privacy in relation to other coins. For instance, in the case of Z-cash, there are two types of addresses: private and transparent ones<sup>244</sup>. If a transaction is performed from a transparent address to another transparent address, the addresses of the parties and the amount of the transaction will be publicly visible<sup>245</sup>. If a transaction is performed from a private address to another private address, the public blockchain will indicate that a transaction has happened and the amount of fees paid, but it will encrypt the addresses of the parties involved and the amount of the transaction itself<sup>246</sup>. As for Monero, this cryptocurrency ecosystem has technological features in place that hide the sender, the receiver and the amount of the transaction<sup>247</sup>. The addresses in Monero are concealed by using one-time automatic addresses for each transaction<sup>248</sup>.

#### **4.2.1. How anonymity can enable money laundering by means of cryptocurrencies**

In September 2020, the FATF issued a guidance indicating a list of red flags for money laundering and terrorist financing associated with the use of virtual assets<sup>249</sup>. That Guidance is based on the analysis of over a hundred cases reported by jurisdictions between 2017 and 2020 – indicating that the presence of one or more of these red flags does not always translate into the existence of criminal activities<sup>250</sup>. There might be legitimate economic reasons explaining the event of the situations regarded as red flags<sup>251</sup>. However, once one or more of these red flags are encountered, this could indicate that the transactions with this client require further monitoring<sup>252</sup>.

---

<sup>242</sup> ‘Zcash Basics — Zcash Documentation 4.5.1 Documentation’, accessed 5 October 2021, [https://zcash.readthedocs.io/en/latest/rtd\\_pages/basics.html](https://zcash.readthedocs.io/en/latest/rtd_pages/basics.html).

<sup>243</sup> The Monero Project, ‘About Monero’, [getmonero.org](https://www.getmonero.org/resources/about/index.html), The Monero Project, accessed 5 October 2021, <https://www.getmonero.org/resources/about/index.html>.

<sup>244</sup> ‘Zcash Basics — Zcash Documentation 4.5.1 Documentation’.

<sup>245</sup> Ibid.

<sup>246</sup> Ibid.

<sup>247</sup> The Monero Project, ‘What Is Monero (XMR)?’, [getmonero.org](https://www.getmonero.org/get-started/what-is-monero/index.html), The Monero Project, accessed 27 November 2021, <https://www.getmonero.org/get-started/what-is-monero/index.html>.

<sup>248</sup> Ibid.

<sup>249</sup> FATF, ‘Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets’ (Paris, 2020), <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html>.

<sup>250</sup> Ibid., 4.

<sup>251</sup> Ibid.

<sup>252</sup> Ibid.

In this document, there is a section dedicated to red flags related to anonymity<sup>253</sup>. The guidance indicates that there are vulnerabilities in the underlying technology of cryptocurrencies (i.e., blockchain) that facilitate anonymity<sup>254</sup>. However, some of the red flag indicators related to anonymity are behaviours that normal users might resort to as protection mechanisms. For instance, the report presents the use of offline wallets as a red flag, but that is a practice many users adopt to protect their funds from hacking attacks<sup>255</sup>. Similarly, transacting more than one type of virtual cryptocurrencies, mainly using enhanced anonymity cryptocurrencies, raises a red flag<sup>256</sup>. Yet, it is usual for cryptocurrency enthusiasts to be “simply” interested in diversifying their portfolio.

For the purposes of the following analysis, the red flags included in the FATF guidance are divided into five categories: 1) AECs; 2) peer-to-peer transactions; 3) tumbler services, 4) cryptocurrency’s design; and 5) red flags that are independent of cryptocurrency’s design. That categorisation should enable the further exploration of the money laundering risks associated with anonymity by means of cryptocurrencies.

#### **a. Anonymity Enhanced Cryptocurrencies (AEC)**

According to the FATF Guidance, it is necessary to pay attention to customers transacting with AECs. It is considered suspicious behaviour to transact with two or more types of cryptocurrencies, especially when one is an AEC<sup>257</sup>. Besides this, moving transparent cryptocurrencies (e.g., bitcoin) to a centralised exchange and immediately trading it for an AEC is deemed suspicious<sup>258</sup>. The use of AECs has increased among enthusiasts of cryptocurrencies that are interested in being protected from law enforcement surveillance<sup>259</sup>. Cybercriminals have been increasingly requesting ransom in AECs<sup>260</sup>.

---

<sup>253</sup> Ibid., 9.

<sup>254</sup> Ibid.

<sup>255</sup> Ibid., 9–10.

<sup>256</sup> Ibid., 9.

<sup>257</sup> Ibid.

<sup>258</sup> Ibid.

<sup>259</sup> Sean Foley, Jonathan R Karlsen, and Tālis J Putniņš, ‘Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?’, *The Review of Financial Studies* 32, no. 5 (1 May 2019): 1807, <https://doi.org/10.1093/rfs/hhz015>.

<sup>260</sup> FinCEN, ‘Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021’, Financial Trend Analysis, 2021, 9.

## **b. Peer-to-peer transactions**

As explained in the previous sections, cryptocurrencies enable peer-to-peer exchanges. This feature has also concerned FATF. As a general rule, it is considered a red flag to have cryptocurrencies transferred to or from wallets associated with DEXs<sup>261</sup>.

Additionally, the FATF Guidance presents two specific situations involving DEXs that may signal money laundering activities. Financial institutions should beware of unlicensed/unregistered cryptocurrency service providers operating at DEXs<sup>262</sup>. This applies especially to situations where such providers charge fees higher than other exchanges and have a large volume of cryptocurrency transactions<sup>263</sup>. Typically, customers prefer providers that have lower costs. So, it seems illogical that an unlicensed service provider whose price tag is above-market practice would have a sizeable business. The other situation involving DEXs that represents a red flag indicator is when a customer that has a wallet associated with a peer-to-peer platform decides to use a centralised exchange to cash out an unusual sum, this could be an indicator of money laundering to the FATF as well<sup>264</sup>.

## **c. Tumbler services (also referred to as mixes, mixers and mixing services)**

Tumbler services mix transactions from numerous users to anonymise the relations between senders and recipients<sup>265</sup>. Customers using these services could be interested in hiding the relation of the funds transacted with known marketplaces of illegal goods<sup>266</sup>. Thus, the use of wallets that have been associated with tumblers is regarded as a red flag indicator<sup>267</sup>.

---

<sup>261</sup> FATF, 'Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets', 9.

<sup>262</sup> Ibid.

<sup>263</sup> Ibid.

<sup>264</sup> Ibid.

<sup>265</sup> Malte Möser, Rainer Böhme, and Dominic Breuker, 'An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem', in *2013 APWG ECrime Researchers Summit*, 2013, 2, <https://doi.org/10.1109/eCRS.2013.6805780>.

<sup>266</sup> FATF, 'Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets', 10.

<sup>267</sup> Ibid.

#### **d. Cryptocurrency's design**

FATF also expresses concerns about cryptocurrencies that do not have documented explanations about their design<sup>268</sup>. The lack of information about that matter could indicate that the coin is linked to frauds such as Ponzi schemes<sup>269</sup>. This can relate to ICOs, which as mentioned above (Section 4), can be exploited by money launderers.

OneCoin is an example of a cryptocurrency without proper information about the design that turned out to be a fraud<sup>270</sup>. Ruja Ignatova, the owner of OneCoin, alleged that she created a cryptocurrency that would soon be more popular than Bitcoin<sup>271</sup>. She convinced people all over the world to invest money totalling 4 billion euros in investments<sup>272</sup>. However, the cryptocurrency has never really existed and the company was operating a Ponzi scheme. The whereabouts of Ruja Ignatova have been unknown since October 2017<sup>273</sup>.

#### **e. Red flags independent of the cryptocurrency design**

The previous four categories are related to the design of cryptocurrencies, but the FATF also highlights some anonymity red flags that are not related to cryptocurrency design. More specifically, cryptocurrency service providers should also beware of clients who registered websites using mechanisms to hide the identity of the website's owner, or using proxy services<sup>274</sup>. The same red flag indicator also alludes to websites registered through domain registrars, i.e., services that manage the registration of internet domains, that do not disclose the domain name's owner<sup>275</sup>. In all those situations, there is no information on the actual owner of the website – fact possibly meaning that this client is trying to increase his/her anonymity.

There are also red-flag indicators related to IP addresses. IP addresses constitute a very important source of information for law enforcement purposes. For instance, it was through the IP address that law enforcement agencies were able to determine the location

---

<sup>268</sup> Ibid.

<sup>269</sup> Ibid.

<sup>270</sup> 'Cryptoqueen: How This Woman Scammed the World, Then Vanished', *BBC News*, 24 November 2019, sec. Stories, <https://www.bbc.com/news/stories-50435014>.

<sup>271</sup> Ibid.

<sup>272</sup> Ibid.

<sup>273</sup> Ibid.

<sup>274</sup> FATF, 'Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets', 10.

<sup>275</sup> Ibid.

of the creator of Silk Road, Ross Ulbricht<sup>276</sup>. Cryptocurrency service providers have to monitor clients using IP addresses related to services that enable anonymous communications, such as VPNs and encrypted e-mails<sup>277</sup>. Moreover, it is considered a red flag indicator if several cryptocurrency wallets that do not seem to be related are operated from the same IP address<sup>278</sup>. According to the FATF Guidance, this behaviour could indicate that an individual has created shell wallets to hide the connexion among the accounts<sup>279</sup>.

In conclusion, this last category refers mainly to mechanisms that can increase anonymity by perpetrators but are not directly related to the blockchain technology. The previous categories are more representative of how the technology of cryptocurrencies can enable money laundering. The use of DEXs, tumblers, and AECs are situations that can be explored by money launderers. Additionally, ICOs can be explored by criminals as the lack of explanation on its design can hide a relation to criminal activities.

#### **4.3. Increased popularity of cryptocurrencies among criminals**

Cryptocurrencies became more popular in 2012, particularly on the Dark Web, where they have been employed as means of payment for drugs, stolen goods and other illicit products and services<sup>280</sup>. Bitcoin allows criminals to conclude transactions in a quicker and cheaper manner than the transactions performed in the financial systems<sup>281</sup>. An international transaction that could take a couple of days, going through one or more intermediary banks, may be completed in an hour in bitcoin.

Through the analysis of millions of unknown Bitcoin addresses composing 2,850 grouped approximations of business entities and by analysing its interaction with a smaller known set of clusters, Tasca *et al.* were able to separate transactions that took place between 2009 and 2015 in four business categories: mining pools, exchanges, online gambling, and black markets. According to these studies, there are three main

---

<sup>276</sup> Tim Hume, 'How the FBI Caught Ross Ulbricht, Alleged Creator of Silk Road - CNN', *CNN*, 5 October 2013, <https://edition.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/index.html>.

<sup>277</sup> FATF, 'Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets', 10.

<sup>278</sup> Ibid.

<sup>279</sup> Ibid.

<sup>280</sup> Paolo Tasca, Shaowen Liu, and Adam Hayes, 'The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment Relationships', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 1 July 2016), 33, <https://doi.org/10.2139/ssrn.2808762>. Ibid.

<sup>281</sup> Anastasia Sotiropoulou and Dominique Guégan, 'Bitcoin and the Challenges for Financial Regulation', *Capital Markets Law Journal* 12, no. 4 (1 October 2017): 467–68, <https://doi.org/10.1093/cmlj/kmx037>.



periods of activity in the Bitcoin network<sup>282</sup>. The first period from 2009 to early 2012 is called “proof-of-concept” and is the beginning of the network when there were not many commercial activities<sup>283</sup>. After that initial stage, criminals, attracted by the lack of legal oversight and the pseudonym, gained interest in Bitcoin<sup>284</sup>. This second stage, referred to by the author as the “early adopters” stage lasted from 2012 to late 2013<sup>285</sup>. The criminal activity seems to have had a sudden decrease in 2012 when Silk Road was shut down by authorities<sup>286</sup>. Finally, from late 2013 onwards there is an expansion of legitimate payments completed in the network, and a decrease of criminal activity.<sup>287</sup> This is the third stage of Bitcoin, and it is called “maturation”<sup>288</sup>.

In the beginning, the criminals were mostly attracted by the lack of a central authority and to the (pseudo)anonymity provided by bitcoin as well as by the lack of regulation and legal oversight<sup>289</sup>. The use of Bitcoin for purchasing illegal goods was seemingly reduced when Silk Road, the most famous marketplace for acquiring illegal goods and services, was shut down in late 2013<sup>290</sup>. Before that, there was no regulation worldwide regarding cryptocurrencies and a Guidance issued by the American Financial Crimes Enforcement Network (FinCEN) in March 2013 noted that cryptocurrencies did not have legal status anywhere in the world at the time<sup>291</sup>. It was only in June 2014, when FATF released the first Guidance on cryptocurrencies.

The most innovative component of Bitcoin at the time it was launched was the DLT design; that is, the Bitcoin did not require a central authority to function, maintain integrity and trustworthiness<sup>292</sup>. In a system that includes a central authority, law enforcement authorities/agencies can request information that may lead to the identification and prosecution of criminals. The most popular cryptocurrencies have a public and permissionless design (e.g., Bitcoin and Ethereum)<sup>293</sup>. In a permissionless

---

<sup>282</sup> Tasca, Liu, and Hayes, ‘The Evolution of the Bitcoin Economy’, 37.

<sup>283</sup> Ibid., 33.

<sup>284</sup> Ibid., 33–34.

<sup>285</sup> Ibid.

<sup>286</sup> Ibid., 34.

<sup>287</sup> Ibid., 35.

<sup>288</sup> Ibid., 39.

<sup>289</sup> Ibid., 33.

<sup>290</sup> Ibid., 34.

<sup>291</sup> ‘Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies’ (FinCEN, 18 March 2013), <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>.

<sup>292</sup> Narayanan, ‘Foreword: The Long Road to Bitcoin’.

<sup>293</sup> Nakamoto, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’; ‘What Is Ether (ETH)?’, [ethereum.org](https://ethereum.org), accessed 7 December 2021, <https://ethereum.org>. Nakamoto, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’; ‘What Is Ether (ETH)?’

blockchain, anyone interested in using the network can join, without further identification or background checks<sup>294</sup>. The identity in the blockchain is represented by the addresses and a person can generate an unlimited number of new addresses<sup>295</sup>. This feature can be seen as advantageous to criminals seeking to hide their traces. Unlike financial institutions, these cryptocurrencies do not allow for any KYC before a new user is allowed to perform online transactions.

Besides pseudo-anonymity, lack of central authority oversight shapes the landscape of cryptocurrencies. The transactions performed on the cryptocurrency network are not monitored by a central institution, nor are they easily reversible<sup>296</sup>. Reversing transactions is only possible with the collaboration of a large number of nodes<sup>297</sup>. Therefore, when cybercrimes involving cryptocurrencies take place, law enforcement agents may identify them, but cannot freeze assets that are in cryptocurrency<sup>298</sup>.

Many things have changed with regard to both cryptocurrencies and the way regulators deal with them since the ‘boom’ that occurred on the Dark Web. The grey area that allowed criminals to enjoy certain freedom with cryptocurrency is now considerably smaller, as regulators and central banks have been directing efforts at regulating cryptocurrencies and imposing obligations to entities that conduct business in the area. At EU level, the 5<sup>th</sup> AMLD has imposed obligations on certain cryptocurrency providers (see Section 5.1). The New York State has introduced a license, named BitLicense, for persons that engage in Virtual Currency Business Activity<sup>299</sup>. More drastically, China has decided to impose a ban on cryptocurrencies<sup>300</sup>. The Chinese central bank states that the use of cryptocurrencies can ‘threaten economic stability and disrupt the existing monetary policy framework’<sup>301</sup>.

---

<sup>294</sup> Casino, Dasaklis, and Patsakis, ‘A Systematic Literature Review of Blockchain-Based Applications’, 57.

<sup>295</sup> Narayanan, ‘Introduction to Cryptography and Cryptocurrencies’.

<sup>296</sup> Harish Natarajan, Solvej Krause, and Helen Gradstein, ‘Distributed Ledger Technology and Blockchain’, Working Paper, FinTech Note (Washington, DC: World Bank, 2017), 26, <https://doi.org/10.1596/29053>.

<sup>297</sup> Hileman and Rauchs, ‘2017 Global Blockchain Benchmarking Study’, 17.

<sup>298</sup> ‘Criminals Hide “billions” in Crypto-Cash - Europol’, *BBC News*, 12 February 2018, sec. Technology, <https://www.bbc.com/news/technology-43025787>.

<sup>299</sup> ‘FAQs: Virtual Currency Businesses’, Department of Financial Services, accessed 7 February 2022, [https://www.dfs.ny.gov/apps\\_and\\_licensing/virtual\\_currency\\_businesses/bitlicense\\_faqs](https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/bitlicense_faqs).

<sup>300</sup> Amy Qin and Ephrat Livni, ‘China Cracks Down Harder on Cryptocurrency With New Ban’, *The New York Times*, 24 September 2021, sec. Business, <https://www.nytimes.com/2021/09/24/business/china-cryptocurrency-bitcoin.html>. Ibid.

<sup>301</sup> ‘Authorities Get Clarity on Digital Money’, accessed 7 February 2022, [http://english.www.gov.cn/news/topnews/202108/06/content\\_WS610c91b6c6d0df57f98de1d2.html](http://english.www.gov.cn/news/topnews/202108/06/content_WS610c91b6c6d0df57f98de1d2.html).

Instead of aiming at cryptocurrencies themselves, regulatory efforts at EU level have been focused mostly on entities that enable the exchange of cryptocurrencies for fiat currencies. The EU AML rules apply to all entities that are involved in the exchange of fiat money for cryptocurrencies (and vice versa) – with them being classified as obliged entities<sup>302</sup>. Thus, these entities need to adopt and act in accordance with KYC policies and report suspicious activities to the authorities.

However, under the AMLD, there are still entities that may deal with cryptocurrencies, without being classified as obliged entities. The example of tumblers is maybe the most representative and dangerous case. Tumbler services mix transactions from numerous users to anonymise the relations between senders and recipients<sup>303</sup>. As noted above (see Section 3), the money laundering process is composed of three steps (placement, layering and integration). According to this model, the placement refers to the moment that the money enters the financial system<sup>304</sup>. However, when it comes to cryptocurrency, the money may go through a layering process even before this money reaches the traditional financial system. Tumbler services make it difficult to identify who is the ultimate originator and beneficiary of a certain transaction<sup>305</sup>. After the layering process, the cryptocurrency could be exchanged for fiat money and placed in the financial system while being distanced from its origins. After that, criminals can send cryptocurrencies to virtual service providers overseas. For instance, the FATF report on Virtual Assets Red Flags indicator presents an example in which criminals turned illicit money into cryptocurrencies and immediately transferred the cryptocurrencies to cryptocurrency exchanges in another jurisdiction<sup>306</sup>. The same report indicates that moving cryptocurrencies to a cryptocurrency exchange located in another jurisdiction can be suspicious if there is no relation between the customer and that jurisdiction, or if the jurisdiction is known to have weak AML/CFT regulations<sup>307</sup>.

---

<sup>302</sup> AMLD Art. 2 (1) (g) (h).

<sup>303</sup> Möser, Böhme, and Breuker, 'An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem', 2. Ibid.

<sup>304</sup> Stessens, *Money Laundering*, 84; Levi and Reuter, 'Money Laundering', 311.

<sup>305</sup> Europol, *Cryptocurrencies*, 10.

<sup>306</sup> FATF, 'Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets', 6.

<sup>307</sup> Ibid.

## **5. THE ANTITHESIS BETWEEN KYC AS A MEANS OF PREVENTING MONEY LAUNDERING AND THE ANONYMITY AS A CORE ELEMENT OF CRYPTOCURRENCIES**

KYC measures can stop dirty money from entering financial institutions, as the latter may refuse to accept clients that are known criminals or fail to comply with KYC requirements, *inter alia*, because of their involvement in criminal activities. KYC is also important for repressing money laundering, as banks can, upon request, provide FIUs with information<sup>308</sup>.

The KYC processes are hard to be implemented in the environment of cryptocurrencies. Cryptocurrencies may follow several types of protocols. It is possible to create a cryptocurrency that performs KYC by default. However, the former attempts to create such cryptocurrencies have not been successful (see Section 4.2). As for now, the main cryptocurrencies available allow for pseudo-anonymity and do not have built-in features for identity verification. As seen before, those characteristics may attract most users to the cryptocurrency world. Users interested in less governmental oversight are unlikely to be receptive to KYC processes.

Taking these factors into consideration, there seems to be an antithesis between the nature of cryptocurrencies, and particularly the element of anonymity, and the AML framework, which currently relies a lot on KYC measures.

Section 5.1 focuses on the analysis of the status quo of the AML and whether it addresses all the opportunities for laundering money by means of cryptocurrencies. Section 5.2 analyses EU plans on AML and cryptocurrencies. Finally, section 5.3 considers the necessity of alternatives for addressing the money laundering opportunities enabled by the anonymity in cryptocurrencies.

### **5.1. AML rules ‘meet’ cryptocurrencies**

The EU legislator and the FATF have recently attempted to impose KYC requirements on cryptocurrencies. At EU level, the 5<sup>th</sup> AMLD provides tools for applying KYC processes to cryptocurrencies. Before that, unless a cryptocurrency service provider performed another venture that resulted in his/her classification as an obliged entity, there

---

<sup>308</sup> AMLD Art. 33 (1) (b).

was no obligation to perform KYC of their clients or to report suspicious activities<sup>309</sup>. The 5<sup>th</sup> AML Directive recognizes that virtual currencies<sup>310</sup> can be misused for criminal purposes, especially due to the anonymity features<sup>311</sup>.

However, cryptocurrencies operate in a decentralized way, and there is usually no central authority able to verify and to keep a record of updated information of the users in the chain. Taking this into consideration, the only effective way found for addressing money laundering issues present in cryptocurrencies was to impose obligations to “gatekeepers”<sup>312</sup>, namely the entities that act as intermediates for those wishing to enter the cryptocurrency ecosystem. The updated list of obliged entities includes “providers engaged in exchange services between virtual currencies and fiat currencies” as well as “custodian wallet providers”<sup>313</sup>. As will be shown, this may be enough for filling some of the regulation gaps, but still leaves space that may be exploited for criminal purposes.

The first definition, “providers engaged in exchange services between virtual currencies and fiat currencies”<sup>314</sup>, is enough to include companies that provide cryptocurrency exchange services, such as centralized cryptocurrency exchanges.

The definition provided by the Directive targets one of the forms of cryptocurrency acquisition: the purchase of cryptocurrency with fiat money (fiat-to-crypto exchanges)<sup>315</sup>. Fiat-to-crypto represents an important volume of cryptocurrency exchanges, but it does not cover it all. A lot of the cryptocurrency trades are crypto-to-crypto exchanges<sup>316</sup>.

Nevertheless, this choice leaves an important number of transactions that happen in the chain uncovered. This is remediated by the second definition included in the Directive: custodian wallet providers. Custodian wallet providers provides services to

---

<sup>309</sup> Haffke, Fromberger, and Zimmermann, ‘Cryptocurrencies and Anti-Money Laundering’, 130.

<sup>310</sup> “Virtual currencies” are defined at 5th AMLD Article 1 (2) (d) and at 4th AMLD Article 3 (18) as: “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”. This definition includes cryptocurrencies as defined in this dissertation, although it is somewhat broader than just that.

<sup>311</sup> 5th AMLD. Recitals (8) and (9).

<sup>312</sup> Haffke, Fromberger, and Zimmermann, ‘Cryptocurrencies and Anti-Money Laundering’, 134.

<sup>313</sup> AMLD Art. (1) (g) (h).

<sup>314</sup> AMLD Art. 2 (1) (g).

<sup>315</sup> Haffke et al. divide the cryptocurrency exchanges in crypto-to-fiat and crypto-to-crypto. In the former fiat money is exchanged for crypto, while in the later all currencies involved in the transaction are cryptocurrencies. Haffke, Fromberger, and Zimmermann, ‘Cryptocurrencies and Anti-Money Laundering’.

<sup>316</sup> Lars Haffke, Mathias Fromberger, and Patrick Zimmermann, ‘Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them’, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 3 February 2019), 128, <https://doi.org/10.2139/ssrn.3328064>.

safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies<sup>317</sup>. This definition is enough to include providers of crypto-to-crypto exchanges that offer clients wallets for storing private keys. However, providers that are not custodian wallet providers are still not obliged entities.

All of that applies only in the case of centralized exchanges. The Decentralized Exchanges (also known as DEXs) use automated smart contracts to perform peer-to-peer transactions, that is, they do not require the existence of a third-party, namely of a custodian wallet provider<sup>318</sup>. Those exchanges traditionally do not allow for fiat-to-crypto exchanges<sup>319</sup>. DEXs are mostly non-custodian<sup>320</sup>; that is, they do not store cryptocurrencies on behalf of customers and, thus, those providers do not fall into the scope of the term “custodian wallet providers”. It can be argued that DEXs are ‘providers engaged in exchange services’, as – although they do not perform the exchanges themselves (the exchanges are peer-to-peer) – they provide the platform through which those exchanges take place. Nonetheless, DEXs cannot be seen as obliged entities because they do not provide exchanges to or from fiat currencies.

DEXs are not regulated and those that perform them do not have any obligations under the EU AML legislation. These providers are famous among crypto enthusiasts for not performing KYC. The increased anonymity makes those providers the perfect option for clients interested in avoiding government surveillance, potentially attracting the attention of criminals. Future reviews to the EU AML framework should take these providers into consideration as the transacted volumes (sum considering the amount bought and the amount sold) in only 24 hours can easily reach two billion dollars for only one DEX. On this date (November 9th, 2021), the volume transacted only by dYdX (the biggest Decentralized Exchange by volume according to the transactions performed on that day) reached 2,683,050,424 dollars. Uniswap (V3) and PancakeSwap (V2) were

---

<sup>317</sup> AMLD Art. 3 (19).

<sup>318</sup> Warren and Bandali, ‘0x: An Open Protocol for Decentralized Exchange on the Ethereum Blockchain’; ‘What Are Decentralized Exchanges, and How Do DEXs Work?’, Cointelegraph, accessed 9 November 2021, <https://cointelegraph.com/defi-101/what-are-decentralized-exchanges-and-how-do-dexs-work>.

<sup>319</sup> Recently, in June 2021, DEX0x has announced the creation of an aggregator to allow buying crypto with fiat currencies through its DEX platform. Yet this should be seen as an exception, as it is not the standard for DEXs. Danny Organ, ‘Matcha x MoonPay: Your Onramp to DeFi’, Matcha, 7 June 2021, <https://www.matcha.xyz/blog/matcha-moonpay>.

<sup>320</sup> Warren and Bandali, ‘0x: An Open Protocol for Decentralized Exchange on the Ethereum Blockchain’; ‘What Are Decentralized Exchanges, and How Do DEXs Work?’

respectively the second and third biggest DEXs and both had volumes higher than 2 billion dollars.<sup>321</sup>

Tumblers are another controversial type of service that does not fall into the scope of the AMLD. Tumblers hide the connexion between the transmitting address and the receiving address<sup>322</sup>. This activity resembles the layering stage of money laundering activities, which could create suspicions as to the lawfulness of the services. Users of tumbler services may be ultimately interested in hiding dirty money, but there are legitimate reasons for a user to wish to hide its footpath in the blockchain. In the blockchain, the transactions are stored in a public database, and it is perfectly legitimate for someone to wish to conceal its transaction history from a counterparty<sup>323</sup>. For instance, if a merchant receives bitcoin as payment for sales, it is necessary to disclose his/her address. The merchant could be interested in using a tumbler script so that his/her clients cannot access transactions s(he) performed. Still, this service is at very high risk of being misused by money launderers. In fact, in 2020, criminal charges were pressed against an individual suspected of running a tumbler service named Helix<sup>324</sup>. Helix provided mixing services for AlphaBay<sup>325</sup> – a dark web marketplace that offered products such as drugs, weapons, malware, and illegal pornography<sup>326</sup>. The prosecutors claim that the service was used to launder more than three hundred million dollars in bitcoin<sup>327</sup>. The suspect pleaded guilty to charges of conspiracy to launder money<sup>328</sup>.

The Directive does not take into consideration the possibility of acquiring cryptocurrency tokens through mining. Individuals and entities that engage in mining are not obliged entities under the AMLD. The miners are responsible for validating transactions on the chain. They are compensated for the service with recently created tokens as well as service fees. It can be argued that miners are service providers, but they do not fit in the category of “providers engaged in exchange services between virtual currencies and fiat currencies” as they do not exchange the tokens for fiat currency. Those

---

<sup>321</sup> ‘Top Cryptocurrency Decentralized Exchanges Ranked’, CoinMarketCap, accessed 9 November 2021, <https://coinmarketcap.com/rankings/exchanges/dex/>.

<sup>322</sup> Möser, Böhme, and Breuker, ‘An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem’, 2.

<sup>323</sup> Haffke, Fromberger, and Zimmermann, ‘Cryptocurrencies and Anti-Money Laundering’, 136.

<sup>324</sup> FATF, ‘Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets’, 11.

<sup>325</sup> Ibid. Ibid.

<sup>326</sup> Foley, Karlsen, and Putniņš, ‘Sex, Drugs, and Bitcoin’, 1807.

<sup>327</sup> Mengqi Sun, ‘Operator of Helix Bitcoin “Mixer” Pleads Guilty’, *Wall Street Journal*, 18 August 2021, sec. C Suite, <https://www.wsj.com/articles/operator-of-helix-bitcoin-mixer-pleads-guilty-11629328791>.

<sup>328</sup> Ibid.

professionals cannot be classified as “custodian wallet providers” either since they do not keep third-party keys.

The fact that miners are outside of the scope of the Directive is not particularly problematic. It might seem like miners have a lot of power in the chain, as they validate transactions, but the miners do not interact with third-parties in their activity<sup>329</sup>. Although mining is a form of acquiring tokens, the miners themselves are not gatekeepers to enter transactions with cryptocurrencies. Consequently, mining is not an activity that represents an elevated risk in terms of money laundering<sup>330</sup>.

Cryptocurrency tokens can also be acquired in ICOs. ICOs are often used to collect funds, for instance, in the context of crowdfunding, avoiding dealing with traditional credit providers<sup>331</sup>. Although it is possible for issuers to give out, also known as airdrops,<sup>332</sup> tokens freely, most issuers of cryptocurrencies sell newly created tokens using smart contracts often operating in the Ethereum network<sup>333</sup>. Currently, issuers of cryptocurrencies are to be seen as obliged entities only if they provide ways to acquire the tokens with fiat money. If so, they can be classified as “providers engaged in exchange services between virtual currencies and fiat currencies”<sup>334</sup>. If the issuer of cryptocurrency decides that one can only acquire cryptocurrencies using other cryptocurrencies, then it falls out of the scope of the AMLD. Freshly created tokens could represent an opportunity for money launderers to hide the source of their funds. Thus, even when it does not involve fiat currency, ICOs should be a matter of concern for legislators.

## **5.2. EU future initiatives on AML and Cryptocurrencies**

There are some ongoing plans in the EU aiming to address AML issues arising from new and emerging technologies and cryptocurrencies in particular. This Section is

---

<sup>329</sup> Valentina Covolo, ‘The EU Response to Criminal Misuse of Cryptocurrencies: The Young, Already Outdated 5th Anti-Money Laundering Directive’, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 13 December 2019), 16, <https://doi.org/10.2139/ssrn.3503535>.

<sup>330</sup> Haffke, Fromberger, and Zimmermann, ‘Cryptocurrencies and Anti-Money Laundering’, 137–38. Ibid.

<sup>331</sup> Barone and Masciandaro, ‘Cryptocurrency or Usury?’, 242.

<sup>332</sup> ‘Crypto Airdrops List December 2021 » Find Free Airdrops & Bounties!’, [airdrops.io](https://airdrops.io/), accessed 6 December 2021, <https://airdrops.io/>.

<sup>333</sup> Haffke, Fromberger, and Zimmermann, ‘Cryptocurrencies and Anti-Money Laundering’, 127. Ibid.

<sup>334</sup> It could be argued that issuers of coins, even when accepting fiat for purchasing cryptocurrencies, would not fit in the definition of providers of exchange services because they allow only for trades from fiat to crypto and not the other way round. However, there is nothing in the directive indicating that the entity needs to allow exchanges both ways in order to be obliged. Haffke, Fromberger, and Zimmermann, ‘Cryptocurrencies and Anti-Money Laundering’, 137.



devoted to the EU AML Action Plan and the EU Digital Finance Strategy. Besides presenting the respective draft provisions, it discusses whether those plans can actually solve the issues detected in the previous sections: that is, the issues with DEXs, tumblers and ICOs.

### 5.2.1. The EU AML Action Plan and legislative proposals

There are plans at EU level for amending its regulatory framework to address new trends of money laundering. In May 2020, the European Commission adopted an action plan that included six pillars for ‘a comprehensive Union policy on preventing money laundering and the financing of terrorism’<sup>335</sup>. Those included:

- “- ensuring the effective implementation of the existing EU AML/CFT<sup>336</sup> framework;
- establishing an EU single rule book on AML/CFT;
- bringing about EU level AML/CFT supervision;
- establishing a support and cooperation mechanism for FIUs;
- enforcing Union-level criminal law provisions and information exchange;
- strengthening the international dimension of the EU AML/CFT framework.”<sup>337</sup>

The *first pillar* focuses on ensuring that the current AML framework is effectively implemented. This presupposes ensuring that the AMLD is transposed and implemented across EU Member States, as well as that those have the technical capacity required to implement reforms to address shortcomings in the EU AML structure<sup>338</sup>.

The *second pillar* refers to the creation of a single rulebook on AML in the EU. The Commission argues that the legislation needs to be more precise to avoid divergences in the enactment of the AML legal framework across EU Member States<sup>339</sup>.

The *third pillar* concerns the need for an AML supervisor authority at EU-level. The Commission understands that the EU does not have an adequate structure to address cross-border AML events<sup>340</sup>. An AML supervisor authority should be able to review

---

<sup>335</sup> European Commission, ‘Communication from the Commission on an Action Plan for a Comprehensive Union Policy on Preventing Money Laundering and Terrorist Financing 2020/C 164/06’ (2020), [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XC0513\(03\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XC0513(03)).

<sup>336</sup> Combating the Financing of Terrorism.

<sup>337</sup> European Commission, Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing 2020/C 164/06, 2.

<sup>338</sup> Ibid., 3.

<sup>339</sup> Ibid., 4.

<sup>340</sup> Ibid., 6.

internal policies, monitor risks across the EU, and promote efficient co-operation among competent authorities in the EU<sup>341</sup>. The powers of this supervising authority could be allocated to a new entity or to an existing entity, namely to the European Banking Authority<sup>342</sup>.

The *fourth pillar* suggests setting up an EU-level mechanism for coordinating and supporting FIUs. That mechanism should also promote co-operation among other authorities, such as law enforcement agencies and tax authorities<sup>343</sup>. This should enable the joint analysis in cases where the obliged entities report suspicious events with a cross-border dimension<sup>344</sup>. The Commission suggests that this mechanism could be administered by an existing EU agency or by an EU-level supervisor authority, should such an entity be created<sup>345</sup>.

The *fifth pillar* regards the enforcement of criminal measures at EU-level and promoting information exchange. According to the Commission, it is crucial to have EU-level capacity to prosecute and investigate financial crimes<sup>346</sup>. The Commission highlights the importance of the Anti-Money Laundering Operational Network (hereinafter AMON) for the purposes of facilitating financial investigations<sup>347</sup>. AMON is an informal network with a focus on AML measures that connects law enforcement contacts<sup>348</sup>. The action plan states that the work of AMON should be enhanced, *inter alia*, by means of a budget to work on concrete cases<sup>349</sup>. The Commission also highlights the importance of public-private partnerships (hereinafter PPPs) in this area<sup>350</sup>. The information shared by FIUs and law enforcement agencies to obliged entities might be restricted to money laundering trends, or it might even involve sharing data on suspects. Nonetheless, the exchange of information in PPPs is a complicated subject as it is necessary to comply with data protection legislations<sup>351</sup>. To remediate this issue, the

---

<sup>341</sup> Ibid., 6–7.

<sup>342</sup> Ibid., 7.

<sup>343</sup> Ibid., 9.

<sup>344</sup> Ibid.

<sup>345</sup> Ibid.

<sup>346</sup> Ibid., 10.

<sup>347</sup> Ibid.

<sup>348</sup> ‘International Anti-Money Laundering Operational Network (AMON) Launched’, Europol, accessed 14 January 2022, <https://www.europol.europa.eu/media-press/newsroom/news/international-anti-money-laundering-operational-network-amon-launched>.

<sup>349</sup> European Commission, Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing 2020/C 164/06, 10.

<sup>350</sup> Ibid.

<sup>351</sup> Ibid., 11.

Commission expresses the necessity of sharing good practices for PPPs concerning data protection and fundamental rights<sup>352</sup>.

Finally, the *sixth pillar* refers to strengthening the international dimension of the EU AML framework. International co-operation is essential to address money laundering – considering its global outreach<sup>353</sup>. To enhance co-operation with third-party states, the Commission proposes that the EU Member States should have coordinated positions on FATF Guidelines/Recommendations<sup>354</sup>. It is also suggested that the Commission could embody the function of representing the EU at FATF<sup>355</sup>. Considering the importance of assessing AML risks related to third countries, the Commission also published a new methodology for assessment of high-risk third countries<sup>356</sup>.

Following the six pillars action plan, in July 2021, the Commission presented a package of four legislative proposals to strengthen AML rules in the EU. The package included: 1) a Proposal for a Regulation establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (hereinafter AMLA)<sup>357</sup>; 2) a Proposal for a Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (hereinafter proposal for AMLR)<sup>358</sup>; 3) a Proposal for a Directive 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 (hereinafter proposal for a 6<sup>th</sup> AMLD)<sup>359</sup>; and 4) a Proposal for a Revision of the 2015 Regulation on Transfer of Funds<sup>360</sup> to include the possibility to trace crypto-assets<sup>361</sup>.

---

<sup>352</sup> Ibid.

<sup>353</sup> Ibid.

<sup>354</sup> Ibid.

<sup>355</sup> Ibid.

<sup>356</sup> Ibid., 12.

<sup>357</sup> European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council Establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and Amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010 COM(2021) 421 Final 2021/0240(COD)’ (2021), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0421>.

<sup>358</sup> 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 COM(2021) 420 Final 2021/0239(COD)’ (2021), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420>.

<sup>359</sup> 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 COM(2021) 423 Final 2021/0250(COD)’ (2021), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0423>.

<sup>360</sup> ‘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 (Text with EEA Relevance)’, 141 OJ L § (2015), <http://data.europa.eu/eli/reg/2015/847/oj/eng>.

<sup>361</sup> 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) COM(2021) 422 Final

Out of these legislative proposals, it is necessary to highlight the significance of the AMLR. As seen before (Section 2.2.1), the subject of AML has been traditionally treated with directives at EU level. The Action plan proposes a shift on the subject of AML, where the AML provisions related to the obliged entities are part of AMLR<sup>362</sup>, while the 6<sup>th</sup> AMLD has its scope limited to the provisions that ‘are not suitable to be directly applicable in the form of a regulation’, *inter alia*, the powers and tasks of competent authorities<sup>363</sup>. EU AML Action Plan also proposes the creation of an EU level AML authority, the AMLA<sup>364</sup>. The AMLA could ensure smoother cooperation among FIUs in the EU<sup>365</sup> and it can cooperate with AML authorities in third countries more effectively<sup>366</sup>.

From the point of view of preventing money laundering in cryptocurrencies, in addition to the plans related to AML, the plans related to digital finance should also be taken into consideration. Thus, the following section will provide an overview of the plans related to the Digital Finance Strategy of the European Commission.

### 5.2.2. Digital Finance Strategy and MICA

Considering that financial services have been moving to digital channels, in September 2020, the European Commission adopted a Digital Finance Strategy for the EU<sup>367</sup>. This strategy presents four priorities: 1) removing fragmentation in the EU Digital Single Market<sup>368</sup>; 2) adapting the EU framework to facilitate digital innovation<sup>369</sup>; 3)

---

2021/0241(COD)’ (2021),  
content/EN/TXT/?uri=CELEX%3A52021PC0422.

[https://eur-lex.europa.eu/legal-](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0422)

<sup>362</sup> Proposal for AMLR, Art. 1 (a).

<sup>363</sup> 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 COM(2021) 423 final 2021/0250(COD), 5.

<sup>364</sup> European Commission, Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010 COM(2021) 421 final 2021/0240(COD).

<sup>365</sup> Proposal for AMLA Recital (2).

<sup>366</sup> Proposal for AMLA Recital (62).

<sup>367</sup> European Commission, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU COM/2020/591 Final’ (2020), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591>.

<sup>368</sup> Ibid., 5–8.

<sup>369</sup> Ibid., 9–12.

establishing a common financial data space to promote data-driven innovation in finance<sup>370</sup>; and 3) addressing challenges and risks related with digital transformation<sup>371</sup>.

With respect to the *first priority*, the Commission plans to create interoperable digital identities that will facilitate the on-boarding process for accessing financial services<sup>372</sup>, and highlights the importance of harmonizing AML rules for customer onboarding across the EU<sup>373</sup>. The respective Communication considers introducing a harmonized licensing procedure for areas that are important for digital finance<sup>374</sup>.

The *second priority* of the digital finance strategy involves ensuring that the EU regulatory framework is compatible with innovative technologies<sup>375</sup>. The Commission suggests regular reviews and interpretative guidance to ensure that the EU regulatory framework is “future proof”<sup>376</sup>. In regard to cryptocurrencies, the digital finance strategy includes a Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets (hereinafter Proposal for MiCA)<sup>377</sup>.

In regard to the *third priority*, the Commission argues that it is important to create a ‘common financial data space’ to facilitate access to public and private data<sup>378</sup>. This includes ensuring that financial information is provided in machine-readable formats<sup>379</sup>, encouraging the use of IT tools that could facilitate reporting and supervision<sup>380</sup>, and a Proposal for an open finance framework to be presented mid-2022<sup>381</sup>.

The *fourth priority* recognizes that there are risks associated with digital finance<sup>382</sup>. The Commission suggests adaptations in the EU supervision to address new actors of the financial ecosystem, i.e., technology companies offering financial services<sup>383</sup>.

---

<sup>370</sup> Ibid., 12–14.

<sup>371</sup> Ibid., 14–17.

<sup>372</sup> Ibid., 5.

<sup>373</sup> Ibid., 6.

<sup>374</sup> Ibid., 7.

<sup>375</sup> Ibid., 9.

<sup>376</sup> Ibid., 11.

<sup>377</sup> Ibid., 9.

<sup>378</sup> Ibid., 12.

<sup>379</sup> Ibid., 13.

<sup>380</sup> Ibid.

<sup>381</sup> Ibid., 14.

<sup>382</sup> Ibid.

<sup>383</sup> Ibid., 15.

### 5.2.3. Critical appraisal of the EU plans

As explained above (Section 5.1), there are three types of activities in the cryptocurrency world that enable anonymity but are not fully addressed in the existing EU legal framework: DEXs, ICOs and tumbling. This Section focuses on whether the EU plans for legislative amendments in the area of AML may address the respective issues efficiently.

The first significant change introduced by those plans is the AMLR (see Section 5.2.1). Considering that the issues inherent in the use of cryptocurrencies have a cross-border nature, cooperation among Member States and with third countries is of central importance. Having a Regulation instead of a Directive as the main AML legislation in the EU guarantees that there are no differences in Member States framework caused by the transposition of the Directive<sup>384</sup>. Uniform standards concerning obliged entities among member states is important to avoid a ‘race to the bottom’<sup>385</sup>.

The proposal for an AMLR includes some topics that were previously part of the AMLD, such as the provisions concerning the responsibilities of obliged entities. However, the AMLR provides more detailed instructions on these matters than what is in the AMLD in force. For instance, the AMLD currently in force requires that the obliged entities identify the customer<sup>386</sup>, but this Directive does not provide details of how the identification must be performed. The AMLR, on the other hand, establishes specific instructions for client identification depending on whether the client is a natural person, a legal entity, a trustee of an express trust, or another type of organization<sup>387</sup>.

With regard to cryptocurrencies, the proposal for an AMLR uses the definitions that are included in the proposal for MiCA. Based on these definitions, the proposal for an AMLR extends the list of the obliged entities beyond what is now included in the AMLD currently in force. According to the proposal for an AMLR, “crypto-asset service providers” are included in the list of obliged entities<sup>388</sup>. Those are defined in the proposal for MiCA as “any person whose occupation or business is the provision of one or more

---

<sup>384</sup> 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 COM(2021) 420 final 2021/0239(COD), 5.

<sup>385</sup> Haffke, Fromberger, and Zimmermann, ‘Cryptocurrencies and Anti-Money Laundering’, 138.

<sup>386</sup> AMLD Art. 13 (1) (a).

<sup>387</sup> Proposal for AMLR Art. 18 (1).

<sup>388</sup> Proposal for new Regulation on AML/CFT Art. 3 (3) (g).

crypto-asset services to third parties on a professional basis”<sup>389</sup>. The list of “crypto-asset services” includes:

- ‘(a) the custody and administration of crypto-assets on behalf of third parties;
- (b) the operation of a trading platform for crypto-assets;
- (c) the exchange of crypto-assets for fiat currency that is legal tender;
- (d) the exchange of crypto-assets for other crypto-assets;
- (e) the execution of orders for crypto-assets on behalf of third parties;
- (f) placing of crypto-assets;
- (g) the reception and transmission of orders for crypto-assets on behalf of third parties
- (h) providing advice on crypto-assets’<sup>390</sup>.

That list of activities and obliged entities is significantly broader than the one entailed in the current AMLD, which includes among the obliged entities only providers engaged in exchange services between virtual currencies and fiat currencies<sup>391</sup> and custodian wallet providers<sup>392</sup>. The crypto-assets service providers have obligations under the proposal for AMLR and under MiCA itself. However, an in-depth explanation of the obligations of crypto-assets service providers in MiCA falls outside the scope of this work as it is not directly related to AML. It suffices to say that under MiCA, crypto-asset service providers need an authorisation to operate in the European Union<sup>393</sup>. Apparently, the definition of “crypto-asset services” provided in the proposal for MiCA covers some of the problems we encountered in the AMLD in section 5.1.

The operation of a trading platform for crypto-assets is defined as:

‘managing one or more trading platforms for crypto-assets, within which multiple third-party buying and selling interests for crypto-assets can interact in a manner that results in a contract, either by exchanging one crypto-asset for another or a crypto-asset for fiat currency that is legal tender’<sup>394</sup>.

That definition does not require that the entity operates exchanges directly to be classified as ‘crypto-asset service provider’. According to this definition, it is enough to operate a platform that allows third parties to buy and sell cryptocurrencies. This is the

---

<sup>389</sup> Proposal for MiCA Art. 3 (8).

<sup>390</sup> Proposal for MiCA Art. 3 (9).

<sup>391</sup> AMLD Art. 2 (3) (g).

<sup>392</sup> AMLD Art. 2 (3) (h).

<sup>393</sup> Proposal for MiCA Art.53.

<sup>394</sup> Proposal for MiCA Art. 3 (11).

key definition that serves to address DEXs, because they offer a platform rather than operating the exchanges themselves. In our opinion, this definition guarantees that these entities do fall into the scope of and have obligations under the proposal for AMLR. This definition also appears to be sufficient to include centralized exchanges, whether they offer the possibility of buying and selling cryptocurrencies using fiat money or not.

At first glance, *centralized exchanges* could also fit in the definition for ‘exchange of crypto-assets for other crypto-assets’. Nonetheless, the proposal for MiCA defines it as ‘concluding purchase or sale contracts concerning crypto-assets with third parties against other crypto-assets by using proprietary capital’<sup>395</sup>. Centralized exchanges offer cryptocurrency exchanging services to customers. Since it requires proprietary capital, this definition in fact includes companies that are operating proprietary trading – i.e., trading for direct gains, instead of trading for a commission.

As far as *issuers of ICOs* are concerned, those providers are not included among the ‘crypto-asset service providers’ in MiCA. Instead, those providers are a separate category named ‘issuers of crypto-assets’. Issuers of crypto-assets are defined as ‘a legal person who offers to the public any type of crypto-assets or seeks the admission of such crypto-assets to a trading platform for crypto-assets’<sup>396</sup>. It seems like issuers of ICOs engage in the activity of “placing of crypto-assets”. However, the definition of this activity presupposes that the crypto-assets are not offered to the public<sup>397</sup>.

Issuers of ICOs are not obliged entities under the proposal for AMLR, but they need to observe the obligations in MiCA for issuers of crypto assets<sup>398</sup>. Although the mere act of offering crypto-assets to the public is not a ‘crypto-asset service’, if the issuer of the ICO provides its own platform to buy the tokens, this entity could be classified as a “crypto-asset service provider” as well. In this case, the issuer will have obligations under the AMLR.

Nonetheless, in most cases, ICOs happen through smart contracts<sup>399</sup>. Through the smart contract, the investors can purchase tokens using other cryptocurrencies, without

---

<sup>395</sup> Proposal for MiCA Art. 3 (13).

<sup>396</sup> Proposal for MiCA Art. 3 (6).

<sup>397</sup> ‘[...] placing of crypto-assets’ means the marketing of newly-issued crypto-assets or of crypto-assets that are already issued but that are not admitted to trading on a trading platform for crypto-assets, to specified purchasers and which does not involve an offer to the public or an offer to existing holders of the issuer’s crypto-assets’ Proposal for MiCA Art. 3 (15).

<sup>398</sup> Proposal for MiCA Art. 4 to 14.

<sup>399</sup> Momtaz, ‘Initial Coin Offerings’, 21 May 2020, 8.



the need for an intermediary<sup>400</sup>. If the issuer of crypto-assets does not perform another activity that is classified as a “crypto-asset service”, the entity will have no obligations under the AMLR. Issuers of ICOs will still need to observe the obligations in MiCA for issuers of crypto-assets. One of these obligations refers to the draft of a *white paper* containing details on the issuers<sup>401</sup>, on the project<sup>402</sup>, and on the technological aspects of the ICO<sup>403</sup>. Although these obligations are focused on protecting investors, presenting thorough information about the aspects of the ICOs can prevent the rise of cryptocurrencies that do not have proper explanation on its design. As seen before (Section 4.2.1), the lack of explanation on the design of a cryptocurrency can be an opportunity for money launderers. Considering that this risk is covered, it might be unnecessary to classify these issuers in the list of obliged entities. Moreover, ICOs are an important mechanism for facilitating financing for SMEs<sup>404</sup>, and imposing the obligation to perform KYC on customers that purchase newly created tokens can be burdensome for SMEs, and eventually even defeat the purpose of ICOs.

In conclusion, entities issuing ICOs are not obliged entities per se. They may be, if they provide a platform in which the clients can acquire the newly issued tokens. Nonetheless, the obligations imposed by MiCA incidentally address one of the money laundering risks related to ICOs (lack of explanation on cryptocurrency’s design).

The proposal for MiCA does not address *tumblers*. This type of service is not directly mentioned in the list of ‘crypto-assets service providers’, nor can it be subsumed under any of the activities included in the list. The providers involved in tumbling activities receive cryptocurrencies from a client and transfer them to another address that cannot be traced back to the client’s original address<sup>405</sup>. At first glance, that activity could fit in the category of ‘the execution of orders for crypto-assets on behalf of third parties’, but the definition of the activity presupposes ‘concluding agreements to buy or to sell one or more crypto-assets’<sup>406</sup> and the activity of tumblers does not entail buying and selling cryptocurrency.

---

<sup>400</sup> Paul P. Momtaz, ‘Initial Coin Offerings’, *PLOS ONE* 15, no. 5 (21 May 2020): 8, <https://doi.org/10.1371/journal.pone.0233018>.

<sup>401</sup> Proposal for MiCA Art. 5 (1) (a).

<sup>402</sup> Proposal for MiCA Art. 5 (1) (b).

<sup>403</sup> Proposal for MiCA Art. 5 (1) (e).

<sup>404</sup> OECD, ‘Initial Coin Offerings (ICOs) for SME Financing’, 30.

<sup>405</sup> Möser, Böhme, and Breuker, ‘An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem’, 3.

<sup>406</sup> “[...] the execution of orders for crypto-assets on behalf of third parties’ means concluding agreements to buy or to sell one or more crypto-assets or to subscribe for one or more crypto-assets on behalf of third parties”. Proposal for MiCA Art. 3 (14).

‘Crypto-assets services’ are listed exhaustively. That raises the question of whether the absence of tumblers automatically means that those are not crypto-assets service providers. Should this be the case, then tumblers would have no AML obligations in the EU. Alternatively, the absence of tumblers activities may only indicate that the European Commission considers that this activity yields such high risks that it should not be authorized in the EU. If that is the case, that subject shall be addressed clearly, explaining the risks associated with the activity and including an express prohibition of the activity in the regulation.

### **5.3. How can AML policies address the anonymity in cryptocurrencies effectively?**

Imposing KYC on cryptocurrency presents great challenges because the creation of digital cash has been rooted in the idea of “increased personal privacy” since the very beginning<sup>407</sup>. The two biggest cryptocurrency ecosystems, i.e., Bitcoin and Ethereum, follow a decentralized structure (using DLT) and preclude the identification of users<sup>408</sup>. The Bitcoin and Ethereum networks combined account for 1.5 trillion dollars in market cap. That is over half of the total market cap for cryptocurrencies (2.4 trillion dollars)<sup>409</sup>.

Without a central authority, there is no means to enforce mandatory identification of the users. In a DLT, the reliability of the data is guaranteed by the nodes in it<sup>410</sup>. However, if the nodes were responsible for verifying personal data from users, it could lead to leaks of personal data. Moreover, the nodes would have very limited resources to determine whether the information provided is reliable or not. Thus, it is difficult to guarantee KYC in the structures of decentralized cryptocurrency networks.

There are scholars that propose blockchain-based applications for KYC<sup>411</sup>. Generally, these proposals include a smart contract that would allow users to have a

---

<sup>407</sup> Chaum, ‘Blind Signatures for Untraceable Payments’, 203. Ibid.

<sup>408</sup> Nakamoto, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’; ‘What Is Ether (ETH)?’ Nakamoto, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’; ‘What Is Ether (ETH)?’

<sup>409</sup> ‘Cryptocurrency Prices, Charts And Market Capitalizations’, CoinMarketCap, accessed 7 December 2021, <https://coinmarketcap.com/>.

<sup>410</sup> Natarajan, Krause, and Gradstein, ‘Distributed Ledger Technology and Blockchain’, 2017, 1.

<sup>411</sup> Alex Biryukov, Dmitry Khovratovich, and Sergei Tikhomirov, ‘Privacy-Preserving KYC on Ethereum’, 2018, [https://doi.org/10.18420/blockchain2018\\_09](https://doi.org/10.18420/blockchain2018_09); Diksha Malhotra, Poonam Saini, and Awadhesh Kumar Singh, ‘How Blockchain Can Automate KYC: Systematic Review’, *Wireless Personal Communications*, 25 August 2021, <https://doi.org/10.1007/s11277-021-08977-0>; José Parra Moyano and Omri Ross, ‘KYC Optimization Using Distributed Ledger Technology’, *Business & Information Systems Engineering* 59, no. 6 (December 2017): 411–23, <https://doi.org/10.1007/s12599-017-0504-2>. Biryukov,

unified identity that could be used for different financial services. However, these solutions are directed at simplifying KYC for financial institutions taking advantage of the DLT design. It could be used by cryptocurrency service providers to select clients based on KYC<sup>412</sup>, but it does not solve the issue of clients that wish to remain anonymous, as adhering to this KYC service could only occur on a voluntary basis.

Even if changes are implemented to the EU legal framework to include in the list of obliged entities those providers that were considered as high-risk, that may not result in fewer money laundering by means of cryptocurrency. That is because some of those high-risk entities are already marginal to some extent and might just refuse to comply with the obligations<sup>413</sup>. This is, for instance, the case with tumblers. It is even possible to find tumblers openly marketing themselves to hide your identity from law enforcement bodies<sup>414</sup>. When it comes to centralized cryptocurrency exchanges that perform crypto-to-fiat transactions, there are more incentives for compliance. Since they perform fiat trades, they need to maintain business relationships with banks and financial institutions which would terminate the relationship in case of non-compliance. However, most DEXs do not perform crypto-to-fiat currency and do not have to deal with financial entities in their business activities. Due to that, a decentralized exchange might not see the same value in complying.

Regulators could place even more emphasis on crypto-to-fiat providers and make it mandatory for those entities to have restrictions or stricter CDD with clients that transfer from tumblers, but that would be incredibly challenging for providers and put them in a vulnerable position. There is no simple way for these entities to identify funds coming from addresses linked to tumbler services. Moreover, this approach would ultimately increase the compliance costs for cryptocurrency service providers.

The actors regulating cryptocurrencies walk a thin line, since imposing a lot of obligations and bans might simply push the market to the underground and make it more suitable for crime to happen instead of preventing money laundering events<sup>415</sup>.

---

Khovratovich, and Tikhomirov, 'Privacy-Preserving KYC on Ethereum'; Malhotra, Saini, and Singh, 'How Blockchain Can Automate KYC'; Parra Moyano and Ross, 'KYC Optimization Using Distributed Ledger Technology'.

<sup>412</sup> Biryukov, Khovratovich, and Tikhomirov, 'Privacy-Preserving KYC on Ethereum', 6. Ibid.

<sup>413</sup> Möser, Böhme, and Breuker, 'An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem', 11.

<sup>414</sup> 'How Does Bitcoin Mixer(Tumbler) Actually Work?', accessed 7 February 2022, <https://mixertumbler.org/how-it-works.html>.

<sup>415</sup> Hossein Nabilou, 'How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency', *International Journal of Law and Information Technology* 27, no. 3 (1 September 2019): 271, <https://doi.org/10.1093/ijlit/eaz008>.

A hands-off approach could be beneficial to diminish market volatility<sup>416</sup>. Nonetheless, regulators need to assess whether market stability is, in fact, desirable and if it will bring any real benefits. Cryptocurrencies are already strongly associated to criminal activity (see Section 4.3). Foley *et al.* estimate that 46% of bitcoin transactions are related to criminal activity<sup>417</sup>. Taking that into consideration, less governmental oversight and regulation might lead to more criminal activity related to cryptocurrency and potentially increase money laundering percentages.

The current EU AML legislation regarding cryptocurrencies relies mainly on the gatekeepers that provide an entry from cryptocurrency networks to traditional financial institutions. That approach is appropriate inasmuch as there are limits to imposing regulations inside the networks (see above), and these providers need to maintain relationships with financial institutions; that is, they have more incentives for compliance than service providers do.

The EU legislative plans go a step further as they address some of the issues that are not covered by the AML rules currently in force. However, there are risks of money laundering attached to cryptocurrencies that cannot be fully addressed by means of KYC policies. In regards to activities that represent high money laundering risks, but cannot be tackled by means of imposing KYC duties on obliged entities (e.g., tumbler services, DEXs), it is necessary to invest in data analysis and improve cooperation among authorities that act in the AML framework, including law enforcement agencies, Europol and FIUs.

The blockchain itself is a strong asset that can be used by law enforcement to detect illicit activities<sup>418</sup>. Although identification in the blockchain is limited to addresses, there is other information, which is publicly available in the blockchain, that can be helpful for law enforcement purposes, such as the number of cryptocurrencies transacted and the time of the transaction<sup>419</sup>. This kind of information can complement the material

---

<sup>416</sup> Savva Shanaev et al., ‘Taming the Blockchain Beast? Regulatory Implications for the Cryptocurrency Market’, *Research in International Business and Finance* 51 (1 January 2020): 10, <https://doi.org/10.1016/j.ribaf.2019.101080>.

<sup>417</sup> Foley, Karlsen, and Putniņš, ‘Sex, Drugs, and Bitcoin’, 1827.

<sup>418</sup> Giannis Tziakouris, ‘Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective’, *IEEE Security Privacy* 16, no. 4 (July 2018): 93, <https://doi.org/10.1109/MSP.2018.3111243>.

<sup>419</sup> Neal B. Christiansen and Julia E. Jarrett, ‘Forfeiting Cryptocurrency: Decrypting the Challenges of a Modern Asset’, *Department of Justice Journal of Federal Law and Practice* 67 (2019): 166.

collected in the course of investigations to substantiate the knowledge law enforcement agencies has on a certain suspect<sup>420</sup>.

For instance, in February 2022, the US Department of Justice was able to seize funds stolen in the Bitfinex hack of 2016 (see Section 4)<sup>421</sup>. In this case, according to the press release from the Department of Justice, the suspects have used tumbler services and converted the cryptocurrencies to AEC, among other money laundering techniques to hide their trail<sup>422</sup>. Although it took over five years, law enforcement agencies, in collaboration with the private sector, were able to link the wallet with the stolen funds to two individuals. It is very likely that they have also relied on information collected on the shutdown of AlphaBay (see Section 5.1)<sup>423</sup>.

Investment in data analysis tools for investigating cryptocurrency flows may be costly, but of central importance for addressing money laundering<sup>424</sup>. The EU should develop tools to assist the Europol and national law enforcement agencies in deanonymizing cryptocurrency addresses. For instance, there are data analysis tools that are able to link seemingly unrelated addresses to the same cluster and tools that can identify when addresses that are known or suspected to be connected to illicit activities happen<sup>425</sup>. However, those tools are usually offered by private partners, and we believe that having such tools developed at EU-level could enable better collaboration among authorities.

There is already a tool similar to that proposed here that is employed for other purposes. In 2020, Europol and the EU created a decryption platform operated by the European Cybercrime Centre (EC3)<sup>426</sup>. This platform should assist law enforcement agencies and Europol investigating terrorism, online child sexual abuse and organised

---

<sup>420</sup> Ibid., 167.

<sup>421</sup> ‘Two Arrested for Alleged Conspiracy to Launder \$4.5 Billion in Stolen Cryptocurrency’, 8 February 2022, <https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency>.

<sup>422</sup> Ibid.

<sup>423</sup> ‘Inside the Chess Match That Led the Feds to \$3.6 Billion in Stolen Bitcoin’, *Time*, 10 February 2022, <https://time.com/6146749/cryptocurrency-laundering-bitfinex-hack/>.

<sup>424</sup> Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2021*, 39.

<sup>425</sup> Christiansen and Jarrett, ‘Forfeiting Cryptocurrency’, 167.

<sup>426</sup> ‘Europol and the European Commission Inaugurate New Decryption Platform to Tackle the Challenge of Encrypted Material for Law Enforcement Investigations’, Europol, accessed 28 November 2021, <https://www.europol.europa.eu/newsroom/news/europol-and-european-commission-inaugurate-new-decryption-platform-to-tackle-challenge-of-encrypted-material-for-law-enforcement>. Ibid.

crime<sup>427</sup>. The alternative for decryption, before that tool was launched, was hiring private companies for decryption services<sup>428</sup>.

Although the development of tools for data analysis is expensive, outsourcing the service seems to have higher costs<sup>429</sup>. Additionally, a forensic examination needs to follow strict procedures<sup>430</sup>. Law enforcement agencies can only trust the task of performing forensic examination to trustworthy partners, and finding a partner qualified for the task can be time-consuming<sup>431</sup>. Europol's decrypting platform could diminish the need to trust a private-partner for performing this sensitive task.

One could expect that having Europol's EC3 ahead of this platform can solve the trust issues and reduce costs for law enforcement agencies. However, since the platform was deployed less than a year ago, there is no data available to know if the tool solves these issues yet. If this experience is proven to be successful, Europol could invest in developing a tool following the same model (i.e., a tool operated by Europol and serving all Member States) for investigating cryptocurrency flows.

## 6. CONCLUSION

Cryptocurrencies have been around for over a decade and have become popular among mainstream users. It is questionable whether the newly acquired users of cryptocurrencies are interested in its potential to be used for payment of goods and services, as it was intended in its conception<sup>432</sup>, or whether this increased interest in cryptocurrencies has a speculative nature<sup>433</sup>.

Even though cryptocurrencies only allow for pseudoanonymity, and the main gatekeepers of cryptocurrencies are required to perform KYC checks on their clients in the EU, criminals often find ways to exploit cryptocurrency for money laundering purposes. The main tools criminals can use for laundering money in cryptocurrency

---

<sup>427</sup> 'Europol and the European Commission Inaugurate New Decryption Platform to Tackle the Challenge of Encrypted Material for Law Enforcement Investigations'.

<sup>428</sup> Ethem Ilbiz and Christian Kaunert, 'Europol and Cybercrime: Europol's Sharing Decryption Platform', *Journal of Contemporary European Studies*, 10 November 2021, 1, <https://doi.org/10.1080/14782804.2021.1995707>.

<sup>429</sup> Ibid., 6–7.

<sup>430</sup> Ibid., 8.

<sup>431</sup> Ibid.

<sup>432</sup> Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System'.

<sup>433</sup> Eng-Tuck Cheah and John Fry, 'Speculative Bubbles in Bitcoin Markets? An Empirical Investigation into the Fundamental Value of Bitcoin', *Economics Letters* 130 (1 May 2015): 32–36, <https://doi.org/10.1016/j.econlet.2015.02.029>.

ecosystems are AECs, DEXs, tumblers, and ICOs. The EU planned initiatives on regulating crypto-markets and reforming AML legislation (i.e., Digital Finance Strategy and EU AML Action Plan) address some of those issues, but there are still cryptocurrency activities that yield money laundering risks and are not addressed in the EU plans. This may be related to the fact that the ecosystem of cryptocurrencies poses difficulties that cannot be addressed by means of KYC.

The step that might in fact address AML risks in the cryptocurrency world may be “courageous” investments with a focus on data analysis. Instead of focusing on transposing KYC to cryptocurrencies, which proves to be cumbersome due to their design, law enforcement should take advantage of the record-keeping feature that blockchains possess for identifying money laundering and illicit activities done by the use of cryptocurrencies.

## 7. BIBLIOGRAPHY

- ‘Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies’. FinCEN, 18 March 2013. <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>.
- Arner, Douglas W., Janos Nathan Barberis, and Ross P. Buckley. ‘FinTech, RegTech and the Reconceptualization of Financial Regulation’. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 1 October 2016. <https://papers.ssrn.com/abstract=2847806>.
- Arner, Douglas W., Dirk A. Zetzsche, Ross P. Buckley, and Janos N. Barberis. ‘The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities’. *European Business Organization Law Review* 20, no. 1 (1 March 2019): 55–80. <https://doi.org/10.1007/s40804-019-00135-1>.
- ‘Authorities Get Clarity on Digital Money’. Accessed 7 February 2022. [http://english.www.gov.cn/news/topnews/202108/06/content\\_WS610c91b6c6d0df57f98de1d2.html](http://english.www.gov.cn/news/topnews/202108/06/content_WS610c91b6c6d0df57f98de1d2.html).
- Azaria, Asaph, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. ‘MedRec: Using Blockchain for Medical Data Access and Permission Management’. In *2016 2nd International Conference on Open and Big Data (OBD)*, 25–30. Vienna, Austria: IEEE, 2016. <https://doi.org/10.1109/OBD.2016.11>.
- Barone, Raffaella, and Donato Masciandaro. ‘Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques’. *European Journal of Law and Economics* 47, no. 2 (1 April 2019): 233–54. <https://doi.org/10.1007/s10657-019-09609-6>.
- Biryukov, Alex, Dmitry Khovratovich, and Sergei Tikhomirov. ‘Privacy-Preserving KYC on Ethereum’, 2018. [https://doi.org/10.18420/blockchain2018\\_09](https://doi.org/10.18420/blockchain2018_09).
- BBC News. ““Bitcoin Fraud Cost Me £500,000””, 4 September 2021, sec. Business. <https://www.bbc.com/news/business-58424832>.

- Bloomberg.com. 'Bitcoin Retreats 20% From Record, Joining Risk-Asset Sell-Off', 26 November 2021. <https://www.bloomberg.com/news/articles/2021-11-26/bitcoin-retreats-20-from-all-time-high-set-earlier-in-november>.
- Reuters. 'Bitcoin Worth \$72 Million Stolen from Bitfinex Exchange in Hong Kong', 3 August 2016, sec. Banks. <https://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP>.
- Blockcerts. 'Blockchain Credentials'. Blockcerts. Accessed 29 March 2021. <http://blockcerts.org/>.
- 'Blockchain for Digital Identity - IBM Blockchain | IBM'. Accessed 29 March 2021. <https://www.ibm.com/blockchain/solutions/identity>.
- Brown, Steven David. 'Cryptocurrency and Criminality: The Bitcoin Opportunity'. *The Police Journal: Theory, Practice and Principles* 89, no. 4 (December 2016): 1–13. <https://doi.org/10.1177/0032258X16658927>.
- Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. 'A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues'. *Telematics and Informatics* 36 (1 March 2019): 55–81. <https://doi.org/10.1016/j.tele.2018.11.006>.
- Cassella, Stefan D. 'Toward a New Model of Money Laundering: Is the "Placement, Layering, Integration" Model Obsolete?' *Journal of Money Laundering Control* 21, no. 4 (1 January 2018): 494–97. <https://doi.org/10.1108/JMLC-09-2017-0045>.
- Chaum, David. 'Blind Signatures for Untraceable Payments'. In *Advances in Cryptology*, edited by David Chaum, Ronald L. Rivest, and Alan T. Sherman, 199–203. Boston, MA: Springer US, 1983. [https://doi.org/10.1007/978-1-4757-0602-4\\_18](https://doi.org/10.1007/978-1-4757-0602-4_18).
- Cheah, Eng-Tuck, and John Fry. 'Speculative Bubbles in Bitcoin Markets? An Empirical Investigation into the Fundamental Value of Bitcoin'. *Economics Letters* 130 (1 May 2015): 32–36. <https://doi.org/10.1016/j.econlet.2015.02.029>.
- Christiansen, Neal B., and Julia E. Jarrett. 'Forfeiting Cryptocurrency: Decrypting the Challenges of a Modern Asset'. *Department of Justice Journal of Federal Law and Practice* 67 (2019): 155.
- CipherTrace. 'Cryptocurrency Crime and Anti-Money Laundering Report (2021)'. CipherTrace, August 2021. <https://info.ciphertrace.com/hubfs/CAML%20Reports/Cryptocurrency%20Crime%20and%20Anti-Money%20Laundering%20Report%2c%20August%202021.pdf>.
- Corbet, Shaen, Brian Lucey, Andrew Urquhart, and Larisa Yarovaya. 'Cryptocurrencies as a Financial Asset: A Systematic Analysis'. *International Review of Financial Analysis* 62 (1 March 2019): 1–51. <https://doi.org/10.1016/j.irfa.2018.09.003>.
- Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, 166 OJ L § (1991). <http://data.europa.eu/eli/dir/1991/308/oj/eng>.
- Covolo, Valentina. 'The EU Response to Criminal Misuse of Cryptocurrencies: The Young, Already Outdated 5th Anti-Money Laundering Directive'. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 13 December 2019. <https://doi.org/10.2139/ssrn.3503535>.
- Cox, Dennis. *Handbook of Anti-Money Laundering*. Chichester, West Sussex, United Kingdom: Wiley, 2014.
- BBC News. 'Criminals Hide "billions" in Crypto-Cash - Europol', 12 February 2018, sec. Technology. <https://www.bbc.com/news/technology-43025787>.
- airdrops.io. 'Crypto Airdrops List December 2021 » Find Free Airdrops & Bounties!' Accessed 6 December 2021. <https://airdrops.io/>.



- CoinMarketCap. 'Cryptocurrency Prices, Charts And Market Capitalizations'. Accessed 7 December 2021. <https://coinmarketcap.com/>.
- BBC News. 'Cryptoqueen: How This Woman Scammed the World, Then Vanished', 24 November 2019, sec. Stories. <https://www.bbc.com/news/stories-50435014>.
- Custers, Bart, Jan-Jaap Oerlemans, and Ronald Pool. 'Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies'. *European Journal of Crime, Criminal Law and Criminal Justice* 28, no. 2 (9 July 2020): 121–52. <https://doi.org/10.1163/15718174-02802002>.
- DeVries, Peter D. 'An Analysis of Cryptocurrency, Bitcoin, and the Future' 1, no. 2 (2016): 9.
- 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 - Commission Declaration, 344 OJ L § (2001). <http://data.europa.eu/eli/dir/2001/97/oj/eng>.
- Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance), 309 OJ L § (2005). <http://data.europa.eu/eli/dir/2005/60/oj/eng>.
- 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 (Text with EEA relevance), 141 OJ L § (2015). <http://data.europa.eu/eli/dir/2015/849/oj/eng>.
- 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 (Text with EEA relevance) (2021). <http://data.europa.eu/eli/dir/2015/849/2021-06-30/eng>.
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 119 OJ L § (2016). <http://data.europa.eu/eli/dir/2016/680/oj/eng>.
- Directive (EU) 2018/843 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 (Text with EEA relevance), 156 OJ L § (2018). <http://data.europa.eu/eli/dir/2018/843/oj/eng>.
- Duyne, Petrus C. van, Jackie H. Harvey, and Liliya Y. Gelemerova. *The Critical Handbook of Money Laundering: Policy, Analysis and Myths*. London: Palgrave Macmillan UK, 2018. <https://doi.org/10.1057/978-1-137-52398-3>.
- Ernst & Young. 'EY Research: Initial Coin Offerings (ICOs)', 2018. [https://assets.ey.com/content/dam/ey-sites/ey-com/en\\_gl/topics/banking-and-capital-markets/ey-research-initial-coin-offerings-icos.pdf](https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-research-initial-coin-offerings-icos.pdf).

- European Commission. Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing 2020/C 164/06 (2020). [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XC0513\(03\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XC0513(03)).
- . Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU COM/2020/591 Final (2020). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591>.
- . 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 COM(2021) 423 final 2021/0250(COD) (2021). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0423>.
- . Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010 COM(2021) 421 final 2021/0240(COD) (2021). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0421>.
- . Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast) COM(2021) 422 final 2021/0241(COD) (2021). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0422>.
- . 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 COM(2021) 420 final 2021/0239(COD) (2021). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420>.
- European Union Agency for Fundamental Rights. *Your Rights Matter: Data Protection and Privacy: Fundamental Rights Survey*. LU: Publications Office, 2020. <https://data.europa.eu/doi/10.2811/292617>.
- Europol. *Cryptocurrencies: Tracing the Evolution of Criminal Finances*. LU: Publications Office, 2021. <https://data.europa.eu/doi/10.2813/75468>.
- . *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Luxembourg: Publications Office of the European Union, 2021.
- Europol. ‘Europol and the European Commission Inaugurate New Decryption Platform to Tackle the Challenge of Encrypted Material for Law Enforcement Investigations’. Accessed 28 November 2021. <https://www.europol.europa.eu/newsroom/news/europol-and-european-commission-inaugurate-new-decryption-platform-to-tackle-challenge-of-encrypted-material-for-law-enforcement>.
- Department of Financial Services. ‘FAQs: Virtual Currency Businesses’. Accessed 7 February 2022. [https://www.dfs.ny.gov/apps\\_and\\_licensing/virtual\\_currency\\_businesses/bitlicense\\_faqs](https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/bitlicense_faqs).
- FATF. ‘International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation’. Paris: FATF, 2012. [www.fatf-gafi.org/recommendations.html](http://www.fatf-gafi.org/recommendations.html).
- . ‘Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets’. Paris, 2020. <http://www.fatf-gafi.org/publications/fatfguides/documents/FATF-VirtualAssets-RedFlagIndicators.pdf>.

- [gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html](https://gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html).
- FinCEN. 'Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021'. Financial Trend Analysis, 2021.
- Foley, Sean, Jonathan R Karlsen, and Tālis J Putniņš. 'Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?' *The Review of Financial Studies* 32, no. 5 (1 May 2019): 1798–1853. <https://doi.org/10.1093/rfs/hhz015>.
- Gadinis, Stavros, and Colby Mangels. 'Collaborative Gatekeepers'. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 11 March 2016. <https://papers.ssrn.com/abstract=2746564>.
- Gill, Martin, and Geoff Taylor. 'Preventing Money Laundering or Obstructing Business? Financial Companies' Perspectives on "Know Your Customer" Procedures'. *The British Journal of Criminology* 44, no. 4 (1 July 2004): 582–94. <https://doi.org/10.1093/bjc/azh019>.
- 'Global Denomination: Coin Dev Interview | Bitcoinist.Com', 25 July 2014. <https://bitcoinist.com/global-denomination-coin-dev-interview/>.
- 'Global Denomination (GDN) X11 DigiShield'. Accessed 31 January 2022. <https://bitcointalk.org/index.php?topic=578574.1460>.
- Haffke, Lars, Mathias Fromberger, and Patrick Zimmermann. 'Cryptocurrencies and Anti-Money Laundering: The Shortcomings of the Fifth AML Directive (EU) and How to Address Them'. *Journal of Banking Regulation* 21, no. 2 (1 June 2020): 125–38. <https://doi.org/10.1057/s41261-019-00101-4>.
- . 'Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them'. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 3 February 2019. <https://doi.org/10.2139/ssrn.3328064>.
- Hileman, Garrick, and Michel Rauchs. '2017 Global Blockchain Benchmarking Study'. *SSRN Electronic Journal*, 2017. <https://doi.org/10.2139/ssrn.3040224>.
- . '2017 Global Cryptocurrency Benchmarking Study'. *SSRN Electronic Journal*, 2017. <https://doi.org/10.2139/ssrn.2965436>.
- 'History of the FATF - Financial Action Task Force (FATF)'. Accessed 20 November 2021. <https://www.fatf-gafi.org/about/historyofthefatf/>.
- Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. *Cybercrime and Digital Forensics: An Introduction*. Second edition. London; New York: Routledge, Taylor & Francis Group, 2018.
- 'How Does Bitcoin Mixer(Tumbler) Actually Work?' Accessed 7 February 2022. <https://mixertumbler.org/how-it-works.html>.
- Hume, Tim. 'How the FBI Caught Ross Ulbricht, Alleged Creator of Silk Road - CNN'. *CNN*, 5 October 2013. <https://edition.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/index.html>.
- IAPP-EY. 'IAPP-EY Annual Privacy Governance Report 2021', 2021. [https://iapp.org/media/pdf/resource\\_center/IAPP\\_EY\\_Annual\\_Privacy\\_Governance\\_Report\\_2021.pdf](https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf).
- IBM Corporation. 'Cost of a Data Breach Report 2021', July 2021.
- Ilbiz, Ethem, and Christian Kaunert. 'Europol and Cybercrime: Europol's Sharing Decryption Platform'. *Journal of Contemporary European Studies*, 10 November 2021, 1–14. <https://doi.org/10.1080/14782804.2021.1995707>.

- Time. 'Inside the Chess Match That Led the Feds to \$3.6 Billion in Stolen Bitcoin', 10 February 2022. <https://time.com/6146749/cryptocurrency-laundering-bitfinex-hack/>.
- Europol. 'International Anti-Money Laundering Operational Network (AMON) Launched'. Accessed 14 January 2022. <https://www.europol.europa.eu/media-press/newsroom/news/international-anti-money-laundering-operational-network-amon-launched>.
- Jourová, Věra. 'Strengthened EU Rules to Prevent'. European Commission, July 2018.
- Kim, Kijin, Steven Beck, and Ma Concepcion Latoja. *2021 Trade Finance Gaps, Growth, and Jobs Survey*. Asian Development Bank, 2021. <https://www.adb.org/publications/2021-trade-finance-gaps-growth-jobs-survey>.
- Kollewe, Julia. 'Bitcoin Price Surges to Record High of More than \$68,000'. *The Guardian*, 9 November 2021, sec. Technology. <https://www.theguardian.com/technology/2021/nov/09/bitcoin-price-record-high-cryptocurrencies-ethereum>.
- Kroon, Udo. 'Ma3tch: Privacy and Knowledge: "Dynamic Networked Collective Intelligence"'. In *2013 IEEE International Conference on Big Data*, 23–31, 2013. <https://doi.org/10.1109/BigData.2013.6691683>.
- Lansky, Jan. 'Possible State Approaches to Cryptocurrencies'. *Journal of Systems Integration* 9, no. 1 (31 January 2018): 19–31. <https://doi.org/10.20470/jsi.v9i1.335>.
- Levi, Michael, and Peter Reuter. 'Money Laundering'. *Crime and Justice* 34 (1 January 2006): 289–375. <https://doi.org/10.1086/501508>.
- LexisNexis Risk Solutions. 'The True Cost of AML Compliance – European Survey European Edition', September 2017. <https://risk.lexisnexis.com/global/en/insights-resources/research/the-true-cost-of-aml-compliance-european-survey>.
- Lusthaus, Jonathan. 'Trust in the World of Cybercrime'. *Global Crime* 13, no. 2 (1 May 2012): 71–94. <https://doi.org/10.1080/17440572.2012.674183>.
- Malhotra, Diksha, Poonam Saini, and Awadhesh Kumar Singh. 'How Blockchain Can Automate KYC: Systematic Review'. *Wireless Personal Communications*, 25 August 2021. <https://doi.org/10.1007/s11277-021-08977-0>.
- McNamee, Michael Sheils. 'HSE Cyber-Attack: Irish Health Service Still Recovering Months after Hack'. *BBC News*, 5 September 2021, sec. Europe. <https://www.bbc.com/news/world-europe-58413448>.
- Milano, Annaliese. 'A Non-Anonymous Stablecoin? Saga Launches With Big-Shot Advisor Team', 22 March 2018. <https://www.coindesk.com/markets/2018/03/22/a-non-anonymous-stablecoin-saga-launches-with-big-shot-advisor-team/>.
- Mitsilegas, Valsamis. 'New Forms of Transnational Policing: The Emergence of Financial Intelligence Units in the European Union and the Challenges for Human Rights: Part 1'. *Journal of Money Laundering Control* 3, no. 2 (1 January 1999): 147–60. <https://doi.org/10.1108/eb027226>.
- Mitsilegas, Valsamis, and Niovi Vavoula. 'The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law'. *Maastricht Journal of European and Comparative Law* 23, no. 2 (1 April 2016): 261–93. <https://doi.org/10.1177/1023263X1602300204>.
- Momtaz, Paul P. 'Initial Coin Offerings'. *PLOS ONE* 15, no. 5 (21 May 2020): e0233018. <https://doi.org/10.1371/journal.pone.0233018>.

- . ‘Initial Coin Offerings’. *PLOS ONE* 15, no. 5 (21 May 2020): e0233018. <https://doi.org/10.1371/journal.pone.0233018>.
- ‘Money Laundering - Financial Action Task Force (FATF)’. Accessed 26 October 2021. <https://www.fatf-gafi.org/faq/moneylaundering/>.
- Möser, Malte, Rainer Böhme, and Dominic Breuker. ‘An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem’. In *2013 APWG ECrime Researchers Summit*, 1–14, 2013. <https://doi.org/10.1109/eCRS.2013.6805780>.
- Mouzakiti, Foivi. ‘Cooperation between Financial Intelligence Units in the European Union: Stuck in the Middle between the General Data Protection Regulation and the Police Data Protection Directive’. *New Journal of European Criminal Law* 11, no. 3 (September 2020): 351–74. <https://doi.org/10.1177/2032284420943303>.
- Muller, Wouter H., Christian Kalin, and John G. Goldsmith, eds. *Anti-Money Laundering: International Law and Practice*. Chichester, West Sussex, England ; Hoboken, N.J: John Wiley & Sons / Henley & Partners, 2007.
- Nabilou, Hossein. ‘How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency’. *International Journal of Law and Information Technology* 27, no. 3 (1 September 2019): 266–91. <https://doi.org/10.1093/ijlit/eaz008>.
- Nakamoto, Satoshi. ‘Bitcoin: A Peer-to-Peer Electronic Cash System’, 2008, 9.
- Narayanan, Arvind. ‘Foreword: The Long Road to Bitcoin’. In *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press, 2016.
- . ‘How Bitcoin Achieves Decentralization’. In *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press, 2016.
- . ‘How to Store and Use Bitcoins’. In *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press, 2016.
- . ‘Introduction to Cryptography and Cryptocurrencies’. In *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press, 2016.
- Natarajan, Harish, Solvej Krause, and Helen Gradstein. ‘Distributed Ledger Technology and Blockchain’. Working Paper. FinTech Note. Washington, DC: World Bank, 2017. <https://doi.org/10.1596/29053>.
- . ‘Distributed Ledger Technology and Blockchain’. Working Paper. FinTech Note. Washington, DC: World Bank, 2017. <https://doi.org/10.1596/29053>.
- O’Dwyer, K. J., and D. Malone. ‘Bitcoin Mining and Its Energy Footprint’, 1 January 2014, 280–85. <https://doi.org/10.1049/cp.2014.0699>.
- OECD. ‘Initial Coin Offerings (ICOs) for SME Financing’, 2019. [www.oecd.org/finance/initial-coin-offerings-for-sme-financing.htm](http://www.oecd.org/finance/initial-coin-offerings-for-sme-financing.htm).
- Organ, Danny. ‘Matcha x MoonPay: Your Onramp to DeFi’. Matcha, 7 June 2021. <https://www.matcha.xyz/blog/matcha-moonpay>.
- Ortolani, Pietro. ‘The Impact of Blockchain Technologies and Smart Contracts on Dispute Resolution: Arbitration and Court Litigation at the Crossroads’. *Uniform Law Review*, 16 May 2019, 430–48. <https://doi.org/10.1093/ulr/unz017>.
- Parra Moyano, José, and Omri Ross. ‘KYC Optimization Using Distributed Ledger Technology’. *Business & Information Systems Engineering* 59, no. 6 (December 2017): 411–23. <https://doi.org/10.1007/s12599-017-0504-2>.
- Pidd, Helen. ‘Man Jailed for Kidnapping Boy Who Was Said to Have Made Money from Bitcoin’. *The Guardian*, 18 October 2021, sec. UK news.

- <https://www.theguardian.com/uk-news/2021/oct/18/man-jailed-for-kidnapping-boy-who-was-said-to-have-made-money-from-bitcoin>.
- Pinto, Rohan. 'Council Post: A Blockchain-Based Digital Notary: What You Need To Know'. *Forbes*, 2019. <https://www.forbes.com/sites/forbestechcouncil/2019/11/12/a-blockchain-based-digital-notary-what-you-need-to-know/>.
- Popescu, Andrei. 'Decentralized Finance (DEFI) - the Lego of Finance'. *Social Sciences and Education Research Review* 7, no. 1 (2020): 321–48.
- Qin, Amy, and Ephrat Livni. 'China Cracks Down Harder on Cryptocurrency With New Ban'. *The New York Times*, 24 September 2021, sec. Business. <https://www.nytimes.com/2021/09/24/business/china-cryptocurrency-bitcoin.html>.
- 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 (Text with EEA relevance), 141 OJ L § (2015). <http://data.europa.eu/eli/reg/2015/847/oj/eng>.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), Pub. L. No. 32016R0679, 119 OJ L (2016). <http://data.europa.eu/eli/reg/2016/679/oj/eng>.
- Saiedi, Ed, Anders Broström, and Felipe Ruiz. 'Global Drivers of Cryptocurrency Infrastructure Adoption'. *Small Business Economics* 57, no. 1 (1 June 2021): 353–406. <https://doi.org/10.1007/s11187-019-00309-8>.
- Schneider, Friedrich, and Ursula Windischbauer. 'Money Laundering: Some Facts'. *European Journal of Law and Economics* 26, no. 3 (1 December 2008): 387–404. <https://doi.org/10.1007/s10657-008-9070-x>.
- Securities and Exchange Commission. 'Investor Alert: Bitcoin and Other Virtual Currency-Related Investments', 2014. [https://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia\\_bitcoin.html](https://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html).
- . 'Ponzi Schemes Using Virtual Currencies', 2013. [https://www.sec.gov/investor/alerts/ia\\_virtualcurrencies.pdf](https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf).
- . 'SEC Charges Global Crypto Lending Platform and Top Executives in \$2 Billion Fraud', 2021. <https://www.sec.gov/news/press-release/2021-172>.
- Shanaev, Savva, Satish Sharma, Binam Ghimire, and Arina Shuraeva. 'Taming the Blockchain Beast? Regulatory Implications for the Cryptocurrency Market'. *Research in International Business and Finance* 51 (1 January 2020): 101080. <https://doi.org/10.1016/j.ribaf.2019.101080>.
- Shaw, Audley. 'De-Risking and Remittances in the Caribbean'. Presented at the Small States Forum 2016 - Towards a Resilient and Equitable Future: Opportunities for Financing and Partnerships, Washington DC, 6 October 2016. <https://caribbeanderisking.com/wp-content/uploads/2021/09/Minister-Shaw-De-risking-Speech-IMF-WB-Annual-Mtgs-6-Oct-2016.pdf>.
- Silva, Patrícia Godinho. 'Recent Developments in EU Legislation on Anti-Money Laundering and Terrorist Financing'. *New Journal of European Criminal Law* 10, no. 1 (March 2019): 57–67. <https://doi.org/10.1177/2032284419840442>.
- 'Sögur'. Accessed 31 January 2022. <https://www.sogur.com/>.
- 'Sögur Currency (SGR): Overview | LinkedIn'. Accessed 1 February 2022. <https://www.linkedin.com/company/sogurcurrency/>.

- Sögur. ‘Sögur’s Whitepaper’. Accessed 31 January 2022. <https://www.sogur.com/whitepaper/>.
- Sotiropoulou, Anastasia, and Dominique Guégan. ‘Bitcoin and the Challenges for Financial Regulation’. *Capital Markets Law Journal* 12, no. 4 (1 October 2017): 466–79. <https://doi.org/10.1093/cmlj/kmx037>.
- Stessens, Guy. *Money Laundering: A New International Law Enforcement Model*. 1st ed. Cambridge University Press, 2000. <https://doi.org/10.1017/CBO9780511494567>.
- Sun, Mengqi. ‘Operator of Helix Bitcoin “Mixer” Pleads Guilty’. *Wall Street Journal*, 18 August 2021, sec. C Suite. <https://www.wsj.com/articles/operator-of-helix-bitcoin-mixer-pleads-guilty-11629328791>.
- Tasca, Paolo, Shaowen Liu, and Adam Hayes. ‘The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment Relationships’. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 1 July 2016. <https://doi.org/10.2139/ssrn.2808762>.
- ‘The FATF Recommendations’. Accessed 20 November 2021. <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>.
- The Monero Project. ‘About Monero’. [getmonero.org](https://getmonero.org), The Monero Project. Accessed 5 October 2021. <https://www.getmonero.org/resources/about/index.html>.
- . ‘What Is Monero (XMR)?’ [getmonero.org](https://getmonero.org), The Monero Project. Accessed 27 November 2021. <https://www.getmonero.org/get-started/what-is-monero/index.html>.
- Tidy, Joe. ‘Irish Cyber-Attack: Hackers Bail out Irish Health Service for Free’. *BBC News*, 21 May 2021, sec. Europe. <https://www.bbc.com/news/world-europe-57197688>.
- CoinMarketCap. ‘Top Cryptocurrency Decentralized Exchanges Ranked’. Accessed 9 November 2021. <https://coinmarketcap.com/rankings/exchanges/dex/>.
- ‘Trust in Technology’. HSBC, 2017.
- ‘Two Arrested for Alleged Conspiracy to Launder \$4.5 Billion in Stolen Cryptocurrency’, 8 February 2022. <https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency>.
- United States Department of Justice. ‘Two O.C. Men Agree to Plead Guilty to Securities Fraud Charge for Swindling Investors Through \$1.8 Million Cryptocurrency Offering’, 2 July 2021. <https://www.justice.gov/usao-cdca/pr/two-oc-men-agree-plead-guilty-securities-fraud-charge-swindling-investors-through-18>.
- Tziakouris, Giannis. ‘Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective’. *IEEE Security Privacy* 16, no. 4 (July 2018): 92–94. <https://doi.org/10.1109/MSP.2018.3111243>.
- Vries, Alex de. ‘Bitcoin’s Growing Energy Problem’. *Joule* 2, no. 5 (16 May 2018): 801–5. <https://doi.org/10.1016/j.joule.2018.04.016>.
- Warren, Will, and Amir Bandeali. ‘0x: An Open Protocol for Decentralized Exchange on the Ethereum Blockchain’, 2017.
- Cointelegraph. ‘What Are Decentralized Exchanges, and How Do DEXs Work?’ Accessed 9 November 2021. <https://cointelegraph.com/defi-101/what-are-decentralized-exchanges-and-how-do-dexs-work>.
- ethereum.org. ‘What Is Ether (ETH)?’ Accessed 7 December 2021. <https://ethereum.org>.
- Wilson, Tom. ‘Crime at Crypto “DeFi” Sites Hits \$10.5 Bln in 2021, Research Shows’. *Reuters*, 19 November 2021, sec. Technology. <https://www.reuters.com/technology/crime-crypto-defi-sites-hits-105-bln-2021-research-shows-2021-11-18/>.

- World Bank Group. 'Data Visualization | Identification for Development'. ID4D. Accessed 6 December 2021. <https://id4d.worldbank.org/global-dataset/visualization>.
- Yermack, David. 'Is Bitcoin a Real Currency? An Economic Appraisal'. Working Paper. Working Paper Series. National Bureau of Economic Research, December 2013. <https://doi.org/10.3386/w19747>.
- 'Zcash Basics — Zcash Documentation 4.5.1 Documentation'. Accessed 5 October 2021. [https://zcash.readthedocs.io/en/latest/rtd\\_pages/basics.html](https://zcash.readthedocs.io/en/latest/rtd_pages/basics.html).